McAfee®

VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

Guia do Usuário

Conteúdo

CAPÍTULO 1

Introdução

O McAfee VirusScan Plus oferece segurança proativa para PC para impedir ataques maliciosos, permitindo que você proteja o que considera importante e navegue, faça pesquisas e download de arquivos on-line, com confiança. As classificações de segurança da Web do McAfee SiteAdvisor ajudam você a evitar sites inseguros. Esse serviço também oferece segurança contra ataques diversificados, combinando tecnologias antivírus, anti-spyware e de firewall. O serviço de segurança da McAfee fornece continuamente o software mais recente para que sua proteção nunca fique desatualizada. Agora você pode adicionar e gerenciar segurança em todos os computadores de sua casa. Além disso, o desempenho aprimorado permite que o programa proteja você, sem incomodá-lo.

Neste capítulo

CAPÍTULO 2

McAfee SecurityCenter

O McAfee SecurityCenter permite monitorar o status de segurança do computador, saber instantaneamente se os serviços de proteção contra vírus, spyware, e-mail e firewall do computador estão atualizados e agir sobre possíveis vulnerabilidades de segurança. Ele fornece as ferramentas e os controles de navegação necessários para coordenar e gerenciar todas as áreas de proteção do computador.

Antes de você começar a configurar e gerenciar a proteção do computador, reveja a interface do SecurityCenter e verifique se entende a diferença entre status, categorias e serviços de proteção. Em seguida, atualize o SecurityCenter para garantir que você tenha a proteção mais recente disponível da McAfee.

Após a conclusão das tarefas de configuração iniciais, você utiliza o SecurityCenter para monitorar o status de proteção do computador. Se o SecurityCenter detectar um problema de proteção, ele o alertará para que possa corrigir ou ignorar o problema (dependendo de sua gravidade). Também é possível rever os eventos do SecurityCenter, como alterações na configuração da varredura de vírus.

Observação: O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician.

Neste capítulo

Recursos do SecurityCenter

O SecurityCenter fornece os seguintes recursos:

Status de proteção simplificado

Analise facilmente o status da proteção do computador, verifique se há atualizações e corrija potenciais problemas de proteção.

Upgrades e atualizações automáticos

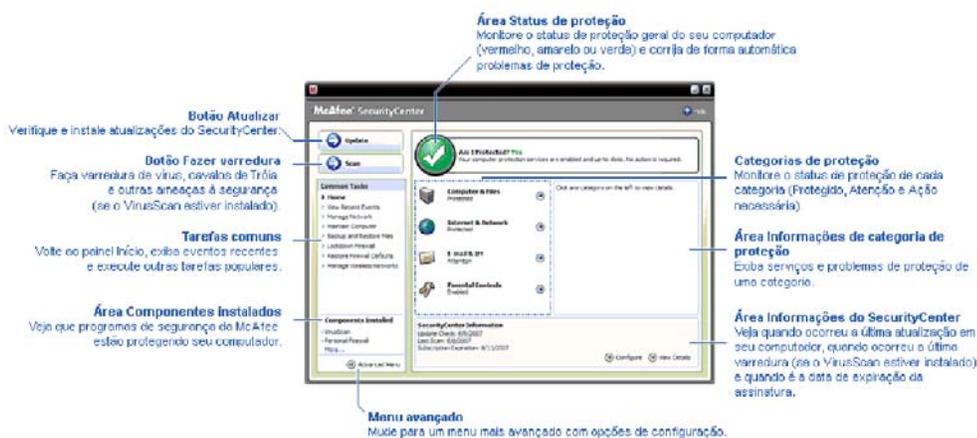
Faça o download e instale automaticamente as atualizações dos programas registrados. Quando há uma nova versão de um programa da McAfee registrado disponível, você a recebe sem custo adicional enquanto sua assinatura é válida, garantindo que você sempre tenha a proteção mais recente.

Alertas em tempo real

Os alertas de segurança notificam sobre epidemias de vírus emergenciais e ameaças à segurança. Também oferecem opções para remover, neutralizar ou aprender mais sobre a ameaça.

CAPÍTULO 3

Usando o SecurityCenter

Antes de começar a usar o SecurityCenter, reveja os componentes e as áreas de configuração que você usará para gerenciar o status da proteção do computador. Para obter mais informações sobre a terminologia usada nesta imagem, consulte Noções básicas sobre o status da proteção (página 8) e Noções básicas sobre as categorias da proteção (página 9). Em seguida, você pode rever as informações de sua conta da McAfee e verificar a validade de sua assinatura.

Neste capítulo

Noções básicas sobre o status da proteção

O status da proteção do computador é mostrado na área de status da proteção, no painel Início do SecurityCenter. Ele indica se o computador está totalmente protegido contra as ameaças de segurança mais recentes e se pode ser influenciado por ataques de segurança externos, outros programas de segurança e programas que acessam a Internet.

O status pode ser vermelho, amarelo ou verde.

Status de proteção	Descrição
Vermelho	Seu computador não está protegido. A área de status da proteção no painel Início do SecurityCenter está em vermelho e indica que o computador não está protegido. O SecurityCenter relata pelo menos um problema de segurança crucial. Para obter a proteção total, é necessário corrigir todos os problemas de segurança cruciais em cada categoria de proteção (o status da categoria do problema é definido como **Ação necessária**, também em vermelho). Para obter informações sobre como corrigir problemas de proteção, consulte Corrigindo problemas de proteção (página 18).
Amarelo	Seu computador está parcialmente protegido. A área de status da proteção no painel Início do SecurityCenter está em amarelo e indica que o computador não está protegido. O SecurityCenter relata pelo menos um problema de segurança não crucial. Para obter proteção total, corrija ou ignore os problemas de proteção não cruciais a cada categoria de proteção. Para obter informações sobre como corrigir ou ignorar problemas de proteção, consulte Corrigindo ou ignorando problemas de proteção (página 17).
Verde	Seu computador está totalmente protegido. A área de status da proteção no painel Início do SecurityCenter está em verde e indica que o computador está protegido. O SecurityCenter não relata nenhum problema de segurança crucial ou não crucial. Cada categoria de proteção lista os serviços que estão protegendo o computador.

Noções básicas sobre categorias de proteção

Os serviços de proteção do SecurityCenter estão divididos em quatro categorias: Computador e arquivos, Rede e Internet, E-mail e mensagens instantâneas e Controles pelos pais. Essas categorias ajudam a procurar e configurar os serviços de segurança que protegem o computador.

Você clica em um nome de categoria para configurar seus serviços de proteção e exibir quaisquer problemas de segurança detectados para esses serviços. Se o problema da proteção do computador for vermelho ou amarelo, uma ou mais categorias exibirão uma mensagem *Ação necessária* ou *Atenção*, indicando que o SecurityCenter tenha detectado um problema dentro da categoria. Para obter mais informações sobre o status da proteção, consulte Noções básicas sobre o status da proteção (página 8).

Categoria da proteção	Descrição
Computador e arquivos	A categoria Computador e arquivos permite configurar os seguintes serviços de proteção: ▪ Proteção contra vírus ▪ Proteção do PUP ▪ Monitores do sistema ▪ Proteção do Windows
Rede e Internet	A categoria Rede e Internet permite configurar os seguintes serviços de proteção: ▪ Proteção de firewall ▪ Proteção de identidade
E-mail e mensagens instantâneas	A categoria E-mail e mensagens instantâneas permite configurar os seguintes serviços de proteção: ▪ Proteção de e-mail ▪ Proteção contra spam
Controles pelos pais	A categoria Controles pelos pais permite configurar os seguintes serviços de proteção: ▪ Bloqueio de conteúdo

Noções básicas sobre serviços de proteção

Os serviços de proteção são os principais componentes do SecurityCenter que você configura para proteger o computador. Os serviços de proteção correspondem diretamente a programas da McAfee. Por exemplo, quando você instala o VirusScan, os seguintes serviços de proteção tornam-se disponíveis: Proteção contra vírus, Proteção de PUP, Monitores do sistema e Proteção do Windows. Para obter informações detalhadas sobre esses serviços específicos de proteção, consulte a Ajuda do VirusScan.

Por padrão, todos os serviços de proteção associados a um programa são ativados quando você instala o programa. Entretanto, um serviço de proteção pode ser desativado a qualquer momento. Por exemplo, se você instalar o Privacy Service, Bloqueio de conteúdo e Proteção de identidade são ativados. Se você não pretender utilizar o serviço de proteção Bloqueio de conteúdo, poderá desativá-lo totalmente. Também pode desativar temporariamente um serviço de proteção enquanto executa tarefas de configuração ou manutenção.

Gerenciando sua conta da McAfee

Gerencie sua conta da McAfee no SecurityCenter, acessando e revisando facilmente as informações da conta e verificando o status atual da assinatura.

Observação: Se você tiver instalado os programas da McAfee de um CD, deverá registrá-los no site da McAfee para configurar ou atualizar a conta da McAfee. Apenas depois você tem direito a atualizações de programas automáticas e regulares.

Gerenciar sua conta da McAfee

Você pode acessar facilmente as informações de sua conta da McAfee (Minha conta) no SecurityCenter.

1 Em **Tarefas comuns**, clique em **Minha conta**.

2 Efetue logon em sua conta da McAfee.

Verificar a assinatura

Você verifica sua assinatura para garantir que ela ainda não tenha expirado.

- Clique com o botão direito no ícone do SecurityCenter, na área de notificação na extrema direita da barra de tarefas, e clique em **Verificar assinatura**.

CAPÍTULO 4

Atualizando o SecurityCenter

O SecurityCenter garante que seus programas da McAfee registrados sejam atuais, verificando e instalando as atualizações on-line a cada quatro horas. Dependendo dos programas instalados e registrados, as atualizações on-line podem incluir as últimas definições de vírus e os upgrades de proteção contra hackers, spams, spywares ou de privacidade. Se desejar verificar as atualizações dentro do período padrão de quatro horas, você poderá fazer isso a qualquer momento. Enquanto o SecurityCenter está verificando as atualizações, você pode continuar a executar outras tarefas.

Embora não seja recomendável, você poderá alterar a maneira que o SecurityCenter verifica e instala as atualizações. Por exemplo, você pode configurar o SecurityCenter para fazer o download, mas não instalar as atualizações nem notificar a você antes do download ou da instalação das atualizações. Também pode desativar a atualização automática.

Observação: Se tiver instalado os programas da McAfee a partir de um CD, você não poderá receber atualizações automáticas e regulares para esses programas, a menos que as registre no site da McAfee.

Neste capítulo

Verificar atualizações

Por padrão, o SecurityCenter verifica automaticamente se há atualizações a cada quatro horas quando o computador está conectado à Internet. Entretanto, se desejar verificar a existência de atualizações dentro desse período, você poderá fazer isso. Se você tiver desativado as atualizações automáticas, será sua responsabilidade verificar regularmente se existem atualizações.

- No painel Início do SecurityCenter, clique em **Atualizar**.

Dica: Você pode verificar se há atualizações sem iniciar o SecurityCenter clicando com o botão direito do mouse no ícone do SecurityCenter, na área de notificação na extrema mais à direita da barra de tarefas, e clicando em **Atualizações**.

Configurar atualizações automáticas

Por padrão, o SecurityCenter verifica automaticamente e instala as atualizações a cada quatro horas quando o computador está conectado à Internet. Se desejar alterar esse comportamento padrão, você poderá configurar o SecurityCenter para fazer download automaticamente das atualizações e notificá-lo quando as atualizações estiverem prontas para serem instaladas ou notificá-lo antes de fazer o download das atualizações.

Observação: O SecurityCenter notifica quando as atualizações estão prontas para serem baixadas ou instaladas usando alertas. A partir dos alertas, você pode fazer download, instalar as atualizações ou adiá-las. Ao atualizar os programas a partir de um alerta, poderá ser solicitado que você verifique sua assinatura antes de fazer o download e instalar. Para obter mais informações, consulte Trabalhando com alertas (página 23).

1 Abra o painel Configuração do SecurityCenter.

   Como?

   1. Em **Tarefas comuns**, clique em **Iniciar**.
   2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.

2 No painel Configuração do SecurityCenter, em **Atualizações automáticas desativadas**, clique em **Ativada** e clique em **Avançado**.

3 Clique em um dos seguintes botões:

   - **Instalar as atualizações automaticamente e notificar-me quando meus serviços estiverem atualizados (recomendável)**
   - **Fazer o download das atualizações automaticamente e notificar-me quando estiverem prontas para serem instaladas**
   - **Notificar-me antes de fazer o download de atualizações**

4 Clique em **OK**.

Desativar atualizações automáticas

Se você desativar as atualizações automáticas, será sua responsabilidade verificar as atualizações regularmente. Do contrário, o computador não terá a proteção de segurança mais recente. Para obter informações sobre a verificação de atualizações manualmente, consulte Verificar atualizações (página 13).

1 Abra o painel Configuração do SecurityCenter.

   Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.

2 No painel Configuração do SecurityCenter, em **Atualizações automáticas ativadas**, clique em **Desativada**.

Dica: Você ativa as atualizações automáticas clicando no botão **Ativada** ou desmarcando **Desativar a atualização automática e permitir a verificação manual de atualizações** no painel Opções de atualização.

CAPÍTULO 5

Corrigindo ou ignorando problemas de proteção

O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Os problemas de proteção cruciais exigem ação imediata e comprometem o status da proteção (alterando a cor para vermelho). Os problemas de proteção não cruciais não exigem ação imediata e podem ou não comprometer o status da proteção (dependendo do tipo de problema). Para obter um status de proteção verde, corrija todos os problemas importantes e corrija ou ignore todos os problemas não cruciais. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician. Para obter mais informações sobre o McAfee Virtual Technician, consulte a ajuda do McAfee Virtual Technician.

Neste capítulo

Corrigindo problemas de proteção

A maioria dos problemas de segurança pode ser corrigida automaticamente. No entanto, alguns problemas exigem que seja tomada alguma ação. Por exemplo, se Proteção de firewall estiver desativada, o SecurityCenter poderá ativá-la automaticamente. No entanto, se não estiver instalada, você deverá fazer isso. A tabela a seguir descreve algumas outras ações que podem ser tomadas ao corrigir problemas de proteção manualmente.

Problema	Ação
Nenhuma varredura completa foi feita no computador nos últimos 30 dias.	Varrer o computador manualmente. Para obter mais informações, consulte a ajuda do VirusScan.
Os arquivos de detecção de assinatura (DATs) estão desatualizados.	Atualizar a proteção manualmente. Para obter mais informações, consulte a ajuda do VirusScan.
Um programa não estão instalado.	Instalar o programa a partir do site da McAfee ou do CD.
Estão faltando componentes em um programa.	Reinstalar o programa a partir do site da McAfee ou do CD.
Um programa não está registrado e não pode receber proteção total.	Registrar o programa no site da McAfee.
Um programa expirou.	Verifique o status de sua conta no site da McAfee.

Observação: Muitas vezes, um único problema de proteção afeta mais de uma categoria de proteção. Nesse caso, corrigir o problema em uma categoria elimina-o de todas as outras categorias de proteção.

Corrigir problemas de proteção automaticamente

O SecurityCenter pode corrigir a maioria dos problemas de proteção automaticamente. As alterações na configuração realizadas pelo SecurityCenter quando ele corrige automaticamente os problemas de proteção não são armazenadas no registro de eventos. Para obter mais informações sobre eventos, consulte Exibindo eventos (página 29).

1 Em **Tarefas comuns**, clique em **Iniciar**.

2 No painel Início do SecurityCenter, na área de status da proteção, clique em **Corrigir**.

Corrigir problemas de proteção manualmente

Se um ou mais problemas de proteção persistirem depois de tentar corrigi-los automaticamente, você poderá corrigir os problemas manualmente.

1 Em **Tarefas comuns**, clique em **Iniciar**.
2 No painel Início do SecurityCenter, clique na categoria de proteção em que o SecurityCenter relata o problema.
3 Clique no link após a descrição do problema.

Ignorando problemas de proteção

Se o SecurityCenter detectar um problema não crucial, você poderá corrigi-lo ou ignorá-lo. Outros problemas não cruciais (por exemplo, se o Anti-Spam ou Privacy Service não está instalado) são automaticamente ignorados. Os problemas ignorados não são mostrados na área de informações de categoria de proteção no painel Início do SecurityCenter, a menos que o status da proteção de seu computador seja verde. Se ignorar um problema, mas decidir posteriormente que ele deve aparecer na área de informações de categoria de proteção mesmo quando o status da proteção de seu computador não for verde, você poderá mostrar o problema ignorado.

Ignorar um problema de proteção

Se o SecurityCenter detectar um problema não crucial que você não pretenda corrigir, será possível ignorá-lo. Ignorá-lo removerá o problema da área de informações de categoria de proteção no SecurityCenter.

1 Em **Tarefas comuns**, clique em **Iniciar**.
2 No painel Início do SecurityCenter, clique na categoria de proteção em que o problema é relatado.
3 Clique no link **Ignorar** ao lado do problema de proteção.

Mostrar ou ocultar problemas ignorados

Dependendo de sua gravidade, você pode mostrar ou ocultar um problema de proteção ignorado.

1 Abra o painel Opções de alerta.

   Como?

   1. Em **Tarefas comuns**, clique em **Iniciar**.
   2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.
   3. Em **Alertas**, clique em **Avançado**.

2 No painel Configuração do SecurityCenter, clique em **Problemas ignorados**.
3 No painel Problemas ignorados, faça o seguinte:
   - Para ignorar um problema, marque a respectiva caixa de seleção.
   - Para relatar um problema na área de informações de categoria de proteção, desmarque a caixa de seleção correspondente.

4 Clique em **OK**.

Dica: Também é possível ignorar um problema clicando no link **Ignorar** ao lado do problema relatado na área de informações de categoria de proteção.

CAPÍTULO 6

Trabalhando com alertas

Alertas são pequenas caixas de diálogo pop-ups que são exibidas no canto inferior direito da tela quando ocorrem determinados eventos do SecurityCenter. Um alerta fornece informações detalhadas sobre um evento, como recomendações e opções para resolver problemas que podem ser associados ao evento. Alguns alertas também contêm links a informações adicionais sobre o evento. Esses links permitem iniciar o site global da McAfee ou enviar informações para a McAfee para solução de problemas.

Há três tipos de alertas: vermelho, amarelo e verde.

Tipo de alerta	Descrição
Vermelho	Um alerta vermelho é uma notificação crucial que requer uma resposta sua. Os alertas vermelhos ocorrem quando o SecurityCenter não pode determinar como corrigir um problema de proteção automaticamente.
Amarelo	Um alerta amarelo é uma notificação não crucial que geralmente requer uma resposta sua.
Verde	Um alerta verde é uma notificação não crucial que não requer uma resposta sua. Os alertas verdes fornecem informações básicas sobre um evento.

Como os alertas reproduzem uma função importante no monitoramento e gerenciamento do status da proteção, você não pode desativá-los. No entanto, pode controlar se determinados tipos de alertas informativos são exibidos e configuram algumas outras opções de alerta (como se o SecurityCenter reproduz um som com um alerta ou exibe a tela de logotipo da McAfee na inicialização).

Neste capítulo

Mostrando e ocultando alertas informativos

Os alertas informativos avisam você quando ocorrem eventos que não apresentam ameaças à segurança do computador. Por exemplo, se você tiver configurado a Proteção de firewall, um alerta informativo será exibido por padrão sempre que for concedido acesso à Internet a um programa do computador. Se você não desejar que um tipo específico de alerta informativo seja exibido, poderá ocultá-lo. Se não desejar que nenhum alerta informativo seja exibido, poderá ocultar todos eles. Também poderá ocultar todos os alertas informativos quando você reproduzir um jogo no modo de tela inteira do computador. Quando você concluir o jogo e sair do modo de tela inteira, o SecurityCenter começará a exibir alertas informativos novamente.

Se ocultar um alerta informativo por engano, você poderá mostrá-lo novamente a qualquer momento. Por padrão, o SecurityCenter mostra todos os alertas informativos.

Mostrar ou ocultar alertas informativos

Você pode configurar o SecurityCenter para mostrar alguns alertas informativos e ocultar outros ou ocultar todos os alertas informativos.

1 Abra o painel Opções de alerta.

   Como?

   1. Em **Tarefas comuns**, clique em **Iniciar**.
   2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.
   3. Em **Alertas**, clique em **Avançado**.

2 No painel Configuração do SecurityCenter, clique em **Alertas informativos**.

3 No painel Alertas informativos, faça o seguinte:

   - Para mostrar um alerta informativo, desmarque a caixa de seleção correspondente.
   - Para ocultar um alerta informativo, marque a respectiva caixa de seleção.
   - Para ocultar todos os alertas informativos, marque a caixa de seleção **Não mostrar alertas informativos**.

4 Clique em **OK**.

Dica: Também é possível ocultar um alerta informativo marcando a caixa de seleção **Não mostrar este alerta novamente** no próprio alerta. Se você fizer isso, poderá mostrar o alerta informativo novamente desmarcando a caixa de seleção adequada no painel Alertas informativos.

Mostrar ou ocultar alertas informativos durante o jogo

Você pode ocultar alertas informativos ao reproduzir um jogo no modo de tela inteira do computador. Quando você concluir o jogo e sair do modo de tela inteira, o SecurityCenter começará a exibir alertas informativos novamente.

1 Abra o painel Opções de alerta.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de alerta, marque a caixa de seleção **Mostrar alertas informativos quando o modo de jogo for detectado**.

3 Clique em **OK**.

Configurando opções de alerta

A aparência e a freqüência dos alertas são configuradas pelo SecurityCenter; entretanto, você pode ajustar algumas opções básicas de alerta. Por exemplo, você pode reproduzir um som com os alertas ou ocultar a exibição do alerta da tela de logotipo quando o Windows iniciar. Você também pode ocultar os alertas que o notificam sobre epidemias de vírus e outras ameaças de segurança na comunidade on-line.

Reproduzir um som com alertas

Se desejar receber uma indicação sonora de que um alerta ocorreu, você poderá configurar o SecurityCenter para reproduzir um som com cada alerta.

1 Abra o painel Opções de alerta.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de alerta, em **Som**, marque a caixa de seleção **Executar um som quando ocorrer um alerta**.

Oculte a tela de logotipo na inicialização.

Por padrão, a tela de logotipo da McAfee é exibida brevemente quando o Windows é iniciado, notificando-o que o SecurityCenter está protegendo o computador. No entanto, você poderá ocultara tela de logotipo se não desejar que ela apareça.

1 Abra o painel Opções de alerta.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de alerta, em **Tela de logotipo**, desmarque a caixa de seleção **Mostrar a tela de abertura da McAfee ao iniciar o Windows**.

Dica: Você pode mostrar a tela de logotipo novamente a qualquer momento marcando a caixa de seleção **Mostrar a tela de abertura da McAfee ao iniciar o Windows**.

Oculte os alertas de epidemias de vírus.

Você pode ocultar os alertas que o notificam sobre epidemias de vírus e outras ameaças de segurança na comunidade on-line.

1 Abra o painel Opções de alerta.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel da direita, em **Informações do SecurityCenter**, clique em **Configurar**.
3. Em **Alertas**, clique em **Avançado**.

2 No painel Opções de alerta, desmarque a caixa de seleção **Alertar-me quando ocorrer uma ameaça de vírus ou segurança**.

Dica: Você pode mostrar os alertas de epidemia de vírus a qualquer momento marcando a caixa de seleção **Alertar-me quando ocorrer um ameaça de vírus ou segurança**.

CAPÍTULO 7

Visualização de eventos

Um evento é uma alteração na ação ou configuração que ocorre dentro de uma categoria de proteção e seus serviços de proteção relacionados. Diferentes serviços de proteção registram diferentes tipos de eventos. Por exemplo, o SecurityCenter registrará um evento se um serviço de proteção estiver ativado ou desativado; a Proteção contra vírus registra um evento cada vez que um vírus é detectado e removido; e a Proteção de firewall registra um evento cada vez que uma tentativa de conexão com a Internet é bloqueada. Para obter mais informações sobre categorias de proteção, consulte Noções básicas sobre categorias de proteção (página 9).

Você pode exibir eventos ao solucionar problemas de configuração e revisar operações executadas por outros usuários. Muitos pais usam o registro de eventos para monitorar o comportamento de seus filhos na Internet. Você exibirá eventos recentes se desejar examinar apenas os últimos 30 eventos que ocorreram. Você exibirá todos os eventos se desejar examinar uma lista completa de todos os eventos que ocorreram. Quando você exibir todos os eventos, o SecurityCenter iniciará o registro de eventos, que classifica os eventos de acordo com a categoria de proteção em que eles ocorreram.

Neste capítulo

Exibir eventos recentes

Você exibirá eventos recentes se desejar examinar apenas os últimos 30 eventos que ocorreram.

- Em **Tarefas comuns**, clique em **Exibir eventos recentes**.

Exibir todos os eventos

Você exibirá todos os eventos se desejar examinar uma lista completa de todos os eventos que ocorreram.

1 Em **Tarefas comuns**, clique em **Exibir eventos recentes**.
2 No painel Eventos recentes, clique em **Exibir registro**.
3 No painel esquerdo do registro de eventos, clique no tipo de eventos a ser exibido.

CAPÍTULO 8

McAfee VirusScan

Os serviços avançados de detecção e proteção do VirusScan defendem você e seu computador contra as ameaças de segurança mais recentes, incluindo vírus, cavalos de Tróia, cookies de rastreamento, spyware, adware e outros programas potencialmente indesejados. A proteção vai além dos arquivos e pastas em seu laptop, atingindo as ameaças de diferentes pontos de entrada, incluindo e-mail, mensagens instantâneas e a Web.

Com o VirusScan, a proteção do computador é imediata e constante (nenhuma administração tediosa é necessária). Enquanto você trabalha, joga, navega pela Web ou verifica seu e-mail, ele é executado no segundo plano, monitorando, examinando e detectando o possível dano em tempo real. Varreduras completas são executadas com base na programação, verificando periodicamente o computador com um conjunto de opções mais sofisticado. O VirusScan oferece a flexibilidade de personalizar esse comportamento, se você desejar; caso contrário, o computador continuará protegido.

Com o uso normal do computador, vírus, worms e outras possíveis ameaças podem infiltrar no computador. Se isso ocorrer, o VirusScan o notificará sobre a ameaça, mas geralmente lidará com ela, limpando ou colocando em quarentena os itens infectados antes que ocorra qualquer dano. Embora seja rara, muitas vezes é necessária alguma ação adicional. Nesses casos, o VirusScan permite que você decida o que fazer (realizar uma nova varredura a próxima vez que iniciar o computador, manter o item detectado o remover o item detectado).

Observação: O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician.

Neste capítulo

Recursos do VirusScan

O VirusScan fornece os recursos a seguir.

Proteção completa contra vírus

Os serviços avançados de detecção e proteção do VirusScan defendem você e seu computador contra as ameaças de segurança mais recentes, incluindo vírus, cavalos de Tróia, cookies de rastreamento, spyware, adware e outros programas potencialmente indesejados. A proteção vai além dos arquivos e pastas e de seu laptop, atingindo as ameaças de diferentes pontos de entrada, incluindo e-mail, mensagens instantâneas e a Web. Nenhuma administração tediosa é necessária.

Opções de varredura com reconhecimento de recursos

Se as varreduras estiverem lenta, você poderá desativar a opção para usar os recursos mínimos do computador, mas lembrar que uma prioridade mais alta será concedida à proteção contra vírus do que a outras tarefas. O VirusScan oferece a flexibilidade de personalizar opções de varredura manuais e em tempo real, se você desejar; caso contrário, o computador continuará protegido.

Reparos automáticos

Se o VirusScan detectar uma ameaça de segurança durante a execução de uma varredura manual ou em tempo real, ele tentará lidar com a ameaça automaticamente, de acordo com o tipo de ameaça. Dessa forma, a maioria das ameaças pode ser detectada e neutralizada sem sua interação. Embora seja raro, o VirusScan em si pode não conseguir neutralizar uma ameaça. Nesses casos, o VirusScan permite que você decida o que fazer (realizar uma nova varredura a próxima vez que iniciar o computador, manter o item detectado o remover o item detectado).

Pausando tarefas em modo de tela inteira

Ao aproveitar coisas como assistir a filmes, executar jogos no computador ou qualquer outra atividade que ocupe a tela inteira do computador, o VirusScan pausa várias tarefas, incluindo atualizações automáticas e varreduras manuais.

Iniciando a proteção contra vírus em tempo real

O VirusScan fornece dois tipos de proteção contra vírus: tempo real e manual. A proteção contra vírus em tempo real monitora constantemente o computador quanto à atividade de vírus, examinando arquivo sempre que você ou seu computador os acessa. A proteção contra vírus manual permite varrer arquivos sob solicitação. Para verificar se o computador permanece protegido contra as ameaças de segurança mais recentes, saia da proteção contra vírus em tempo real e configure uma programação para varreduras manuais mais abrangentes e regulares. Por padrão, o VirusScan executa uma varredura programada uma vez por semana. Para obter mais informações sobre a varredura manual e em tempo real, consulte Fazendo a varredura do computador (página 57).

Embora seja raro, pode haver momentos em que você deseja parar temporariamente a varredura em tempo real (por exemplo, para alterar algumas opções de varredura ou solucionar um problema de desempenho). Quando a proteção contra vírus em tempo real está desativada, o computador não está protegido e o status da proteção do SecurityCenter é vermelho. Para obter mais informações sobre o status da proteção, consulte "Noções básicas sobre o status da proteção" na ajuda do SecurityCenter.

Iniciar a proteção contra vírus em tempo real

Por padrão, a proteção contra vírus em tempo real é ativada e protege o computador contra vírus, cavalos de Tróia e outras ameaças de segurança. Se você desativar a proteção contra vírus em tempo real, deverá ativá-la novamente para ficar protegido.

1 Abra o painel de configuração Computador e arquivos.

Como?

1. No painel esquerdo, clique no **menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador e arquivos**.

2 Em **Proteção contra vírus**, clique em **Ligado**.

Parar a proteção contra vírus em tempo real

Você pode desativar a proteção contra vírus em tempo real temporariamente e especifique quando ela retomar. Você pode retomar automaticamente a proteção após 15, 30, 45 ou 60 minutos, qual o computador reiniciar ou nunca.

1 Abra o painel de configuração Computador e arquivos.

Como?

1. No painel esquerdo, clique no **menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador e arquivos**.

2 Em **Proteção contra vírus**, clique em **Desligado**.

3 Na caixa de diálogo, selecione quando retomar a varredura em tempo real.

4 Clique em **OK**.

CAPÍTULO 9

Iniciando proteção adicional

Além da proteção contra vírus em tempo real, o VirusScan fornece proteção avançada contra scripts, spyware e anexos de mensagens instantâneas e e-mails potencialmente nocivos. Por padrão, a proteção de varredura de script, spyware, e-mail e mensagem instantânea está ativada e protegendo o computador.

Proteção de varredura de script

A proteção de varredura de script detecta scripts potencialmente nocivos e impede-os de serem executados no computador. Ela monitora o computador quanto à atividade de script suspeita, como um script que cria, copia ou exclui arquivos ou abre seu Registro do Windows e alerta-o antes que ocorra qualquer dano.

Proteção contra spyware

A proteção contra spyware detecta spyware, adware e outros programas potencialmente indesejados. Spyware é o software que pode ser secretamente instalado no computador para monitorar seu comportamento, coletar informações pessoas e, até mesmo, interferir no controle do computador instalando software adicional ou redirecionando a atividade do navegador.

Proteção de e-mail

A proteção de e-mail detecta atividade suspeita no e-mail e os anexos que você envia e recebe.

Proteção de mensagem instantânea

A proteção de mensagem instantânea detecta as possíveis ameaças de segurança de anexos de mensagens instantâneas que você recebe. Ela também impede os programas de mensagens instantâneas de compartilhar informações pessoais.

Neste capítulo

Iniciar proteção de varredura de script

Ative a proteção de varredura de script detectar scripts potencialmente nocivos e impedi-los de serem executados no computador. A proteção de varredura de script alerta-o quando um script tenta criar, copiar ou excluir arquivos do computador ou fazer alterações no Registro do Windows.

1 Abra o painel de configuração Computador e arquivos.

Como?

1. No painel esquerdo, clique no **menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador e arquivos**.

2 Em **Proteção de varredura de scripts**, clique em **Ligado**.

Observação: Embora você possa desativar a proteção de varredura de script a qualquer momento, isso deixa o computador vulnerável a scripts nocivos.

Iniciar proteção contra spyware

Ative a proteção contra spyware para detectar e remover spyware, adware e outros programas potencialmente indesejados que reúnam e transmitam informações sem seu conhecimento ou permissão.

1 Abra o painel de configuração Computador e arquivos.

Como?

1. No painel esquerdo, clique no **menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador e arquivos**.

2 Em **Proteção de varredura de scripts**, clique em **Ligado**.

Observação: Embora você possa desativar a proteção contra spyware a qualquer momento, isso deixa o computador vulnerável a programas potencialmente indesejados.

Iniciar proteção de e-mail

Ative a proteção de e-mail para detectar worms, bem como possíveis ameaças em mensagens e anexos de e-mail de entrada (POP3) e saída (SMTP).

1 Abra o painel Configuração de e-mail e mensagens instantâneas.

Como?

1. No painel esquerdo, clique no **menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **E-mail e mensagens instantâneas**.

2 Em **Proteção de e-mail**, clique em **Ligado**.

Observação: Embora você possa desativar a proteção de e-mail a qualquer momento, isso deixa o computador vulnerável a ameaças de e-mail.

Iniciar a proteção para mensagens instantâneas

Ative a proteção para mensagens instantâneas para detectar ameaças de segurança que possam ser incluídas em anexos de mensagens instantâneas.

1 Abra o painel Configuração de e-mail e mensagens instantâneas.

Como?

1. No painel esquerdo, clique no **menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **E-mail e mensagens instantâneas**.

2 Em **Proteção para mensagens instantâneas**, clique em **Ligado**.

Observação: Embora você possa desativar a proteção para mensagens instantâneas a qualquer momento, isso deixa o computador vulnerável a anexos nocivos de mensagens instantâneas.

CAPÍTULO 10

Configurando a proteção contra vírus

O VirusScan fornece dois tipos de proteção contra vírus: tempo real e manual. A proteção contra vírus em tempo real varre os arquivos sempre que são acessados por você ou seu computador. A proteção contra vírus manual permite varrer arquivos sob solicitação. Você pode definir diferentes opções para cada tipo de proteção. Por exemplo, como a proteção em tempo real monitora continuamente seu computador, você pode selecionar determinado conjunto de opções básicas de varredura, reservando um conjunto mais abrangente de opções de varredura para proteção manual sob solicitação.

Neste capítulo

Definindo opções de varredura em tempo real

Quando você inicia a proteção contra vírus em tempo real, o VirusScan usa um conjunto padrão de opções para varrer arquivos; no entanto, você pode alterar as opções padrão para que sejam adequadas às suas necessidades.

Para alterar opções de varredura em tempo real, você deve tomar decisões sobre o que o VirusScan verifica durante uma varredura, bem como os locais e os tipos de arquivo que ele varre. Por exemplo, você pode determinar se o VirusScan verifica se há vírus desconhecidos ou cookies que os sites possam usar para rastrear seu comportamento e se ele examina as unidades de rede mapeadas para o computador ou apenas as unidades locais. Você também pode determinar quais tipos de arquivos são varridos (todos os arquivos ou apenas arquivos e documentos de programas, pois é onde o maior número de vírus é detectado).

Ao alterar opções de varredura em tempo real, você também deve determinar se é importante para seu computador ter a proteção contra a sobrecarga do buffer. Um buffer é uma parte da memória usada para reter temporariamente informações do computador. Sobrecargas de buffer podem ocorrem quando a quantidade de informações que programas ou processos suspeitos armazenam em um buffer excedem a capacidade do buffer. Quando isso ocorre, o computador torna-se mais vulnerável a ataques de segurança.

Definir opções de varredura em tempo real

Você define opções de varredura em tempo real para personalizar o que o VirusScan procura durante uma varredura em tempo real, bem como os locais e tipos de arquivos que ele examina. As opções incluem varredura de vírus desconhecidos e rastreamento de cookies, bem como o fornecimento de proteção contra a sobrecarga do buffer. Você também pode configurar a varredura em tempo real para verificar unidades de rede que são mapeadas para o computador.

1 Abra o painel Varredura em tempo real.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Computador e arquivos**.
3. Na área de informações Computador e arquivos, clique em **Configurar**.
4. No painel de configuração Computador e arquivos, verifique se a proteção contra vírus está ativada e clique em **Avançado**.?

2 Especifique as opções de varredura em tempo real e clique em **OK**.

Para...	Faça isto...
Detectar vírus desconhecidos e novas variantes de vírus conhecidos.	Marque a caixa de seleção **Fazer varredura para vírus desconhecidos usando heurística**.
Detectar cookies.	Marque a caixa de seleção **Fazer varredura e remover cookies de rastreamento**.
Detectar vírus e outras possíveis ameaças em unidades que são conectadas à rede.	Marque a caixa de seleção **Fazer varredura de unidades de rede**.
Proteger o computador contra sobrecargas do buffer.	Marque a caixa de seleção **Ativar proteção contra a sobrecarga do buffer**.
Especificar quais tipos de arquivos em que fará varredura.	Clique em **Todos os arquivos (recomendável)** ou **Apenas arquivos de programa e documentos**.

Configurando opções de varredura manual

A proteção contra vírus manual permite varrer arquivos sob solicitação. Quando você inicia uma varredura manual, o VirusScan verifica se há vírus ou outros itens potencialmente nocivos no computador, usando um conjunto mais abrangente de opções de varredura. Para alterar opções de varredura manual, você deve tomar decisões sobre o que o VirusScan verifica durante uma varredura. Por exemplo, você pode determinar se o VirusScan procura vírus desconhecidos, programas potencialmente indesejados, como spyware ou adware, programas furtivos, como rootkits que podem conceder acesso não autorizado ao computador, e cookies que os sites podem usar para rastrear seu comportamento. Você também deve tomar decisões sobre os tipos de arquivos verificados. Por exemplo, você pode determinar se o VirusScan verifica todos os arquivos ou apenas arquivos de programas e documentos (pois é nesses locais que a maior parte dos vírus é detectada). Também é possível determinar se os arquivos compactados (por exemplo, arquivos .zip) são incluídos na varredura.

Por padrão, o VirusScan verifica todas as unidades e pastas no computador sempre que ele executa uma varredura manual; no entanto, você pode alterar os locais padrão para se adequar às suas necessidades. Por exemplo, você pode fazer a varredura apenas em arquivos de sistema, itens da área de trabalho ou itens na pasta Arquivos de programas críticos. A menos que deseje ser responsável pelo início de cada varredura manual, você poderá configurar uma programação regular para varreduras. As varreduras programadas sempre verificam todo o computador, usando as opções de varredura padrão. Por padrão, o VirusScan executa uma varredura programada uma vez por semana.

Se as varreduras estiverem lentas, considere a possibilidade de desativar a opção para usar os recursos mínimos do computador, mas lembre-se que uma prioridade mais alta será concedida à proteção contra vírus do que a outras tarefas.

Observação: Ao aproveitar coisas como assistir a filmes, executar jogos no computador ou qualquer outra atividade que ocupe a tela inteira do computador, o VirusScan pausa várias tarefas, incluindo atualizações automáticas e varreduras manuais.

Configurar opções de varredura manual

Você define opções de varredura manual para personalizar o que o VirusScan procura durante uma varredura manual, bem como os locais e tipos de arquivos que ele examina. As opções incluem a varredura de vírus desconhecidos, compactações de arquivos, spyware e programas potencialmente indesejados, cookies de rastreamento, rootkits e programas furtivos.

1 Abra o painel Varredura manual.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Computador e arquivos**.
3. Na área de informações Computador e arquivos, clique em **Configurar**.
4. No painel de configuração Computador e arquivos, verifique se a proteção contra vírus está ativada e clique em **Avançado**.
5. Clique em **Varredura manual** no painel Proteção contra vírus.

2 Especifique as opções de varredura manual e clique em **OK**.

Para...	Faça isto...
Detectar vírus desconhecidos e novas variantes de vírus conhecidos.	Marque a caixa de seleção **Fazer varredura para vírus desconhecidos usando heurística**.
Detectar e remover os vírus nos arquivos .zip e em outros arquivos compactados.	Marque a caixa de seleção **Fazer varredura em arquivos .zip e outros arquivos compactados**.
Detectar spyware, adware e outros programas potencialmente indesejados.	Marque a caixa de seleção **Fazer a varredura para spyware e programas potencialmente indesejados**.
Detectar cookies.	Marque a caixa de seleção **Fazer varredura e remover cookies de rastreamento**.
Detectar rootkits e programas furtivos que podem alterar e explorar arquivos do sistema Windows existentes.	Marque a caixa de seleção **Fazer a varredura para rootkits e outros programas furtivos**.

Para...	Faça isto...
Usar menos potência do processador para as varreduras, dando maior prioridade a outras tarefas (como navegar na Internet ou abrir documentos).	Marque a caixa de seleção **Fazer varredura usando o mínimos de recursos do computador**.
Especificar quais tipos de arquivos em que fará varredura.	Clique em **Todos os arquivos (recomendável)** ou **Apenas arquivos de programa e documentos**.

Definir local da varredura manual

Você define o local da varredura manual para determinar onde o VirusScan procura vírus e outros itens nocivos durante uma varredura manual. Você pode varrer todos os arquivos, as pastas e as unidades do computador ou pode restringir a varredura a pastas e unidades específicas.

1 Abra o painel Varredura manual.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Computador e arquivos**.
3. Na área de informações Computador e arquivos, clique em **Configurar**.
4. No painel de configuração Computador e arquivos, verifique se a proteção contra vírus está ativada e clique em **Avançado**.
5. Clique em **Varredura manual** no painel Proteção contra vírus.

2 Clique em **Local padrão para fazer a varredura**.

3 Especifique o local da varredura manual e clique em **OK**.

Para...	Faça isto...
Varrer todos os arquivos e pastas no computador.	Marque a caixa de seleção **(Meu) computador**.
Fazer a varredura de arquivos, pastas e unidades específicas no computador.	Desmarque a caixa de seleção **(Meu) computador** e selecione uma ou mais pastas ou unidades.

Para...	Faça isto...
Fazer varredura dos arquivos essenciais do sistema.	Desmarque a caixa de seleção **(Meu) computador** e marque a caixa **Arquivos de sistema importantes**.

Programar uma varredura

Programe as varreduras para verificar totalmente o computador quanto a vírus e outras ameaças qualquer dia e horário da semana. As varreduras programadas sempre verificam todo o computador, usando as opções de varredura padrão. Por padrão, o VirusScan executa uma varredura programada uma vez por semana. Se as varreduras estiverem lentas, considere a possibilidade de desativar a opção para usar os recursos mínimos do computador, mas lembre-se que uma prioridade mais alta será concedida à proteção contra vírus do que a outras tarefas.

1 Abra o painel Varredura programada.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Computador e arquivos**.
3. Na área de informações Computador e arquivos, clique em **Configurar**.
4. No painel de configuração Computador e arquivos, verifique se a proteção contra vírus está ativada e clique em **Avançado**.
5. Clique em **Varredura programada** no painel Proteção contra vírus.

2 Selecione **Ativar varredura programada**.

3 Para reduzir a quantidade de potência do processador normalmente usada para a varredura, selecione **Fazer varredura usando o mínimo de recursos do computador**.

4 Selecione um ou mais dias.

5 Especifique um horário de início.

6 Clique em **OK**.

Dica: Você pode restaurar a programação padrão clicando em **Redefinir**.

Usando opções de SystemGuards

Os SystemGuards monitoram, registram, relatam e gerenciam alterações potencialmente não autorizadas feitas no Registro do Windows ou em arquivos importantes de sistema no computador. Alterações de registro e arquivo não autorizadas podem danificar seu computador, comprometer sua segurança e danificar arquivos de sistema importantes.

As alterações de registro e arquivo são comuns e ocorrem regularmente no computador. Como muitas são inofensivos, as definições padrão dos SystemGuards são configuradas para fornecer proteção confiável, inteligente e real contra alterações não autorizadas que representam potencial significativo para danos. Por exemplo, quando os SystemGuards detectam alterações que são incomuns e apresentam uma ameaça potencialmente significativa, a atividade é imediatamente relatada e registrada. As alterações mais comuns, mas que ainda representam algum potencial para danos, são apenas registradas. No entanto, o monitoramento para alterações padrão e de baixo risco é desativado por padrão. A tecnologia SystemGuards pode ser configurada para estender a respectiva proteção a qualquer ambiente que você deseje.

Há três tipos de SystemGuards: SystemGuards de programa, SystemGuards do Windows e SystemGuards de navegador.

SystemGuards de programas

Detectam alterações potencialmente não autorizadas no registro do computador e em outros arquivos importantes que são essenciais para o Windows. Esses arquivos e itens de registro importantes incluem instalações do ActiveX, itens de inicialização, ganchos de execução de shell do Windows e carregamentos de atraso do objeto de serviço do shell. Ao monitorar isso, a tecnologia SystemGuards de programa pára os programas ActiveX suspeitos (baixados da Internet), além de spyware e dos programas potencialmente indesejados que podem iniciar automaticamente quando o Windows inicia.

SystemGuards do Windows

Também detectam alterações potencialmente não autorizadas no registro do computador e em outros arquivos importantes que são essenciais para o Windows. Esses itens de registro e arquivos importantes incluem identificadores do menu de contexto, DLLs appInit e o arquivo hosts do Windows. Ao monitorá-los, a tecnologia SystemGuards do Windows ajuda a impedir o computador de enviar e receber informações pessoais ou não autorizadas pela Internet. Também ajuda a bloquear programas suspeitos que trazem alterações indesejadas para a aparência e o comportamento de programas importantes para você e sua família.

SystemGuards de navegador

Assim como os SystemGuards de programa e do Windows, os SystemGuards de navegador detectam alterações potencialmente não autorizadas no registro do computador e em outros arquivos importantes que são essenciais para o Windows. No entanto, os SystemGuards de navegador monitoram as alterações em itens de registro e arquivos importantes, como suplementos, URLs e zonas de segurança do Internet Explorer. Ao monitorá-los, a tecnologia SystemGuards de navegador ajuda a impedir a atividade de navegador não autorizado, como redirecionamento para sites suspeitos, alterações nas configurações e opções do navegador sem seu conhecimento e confiança indesejada de sites suspeitos.

Ativar a proteção de SystemGuards

Ative a proteção de SystemGuards para detectar e alertá-lo de alterações de arquivos e registro do Windows potencialmente não autorizadas no computador. Alterações de registro e arquivo não autorizadas podem danificar seu computador, comprometer sua segurança e danificar arquivos de sistema importantes.

1 Abra o painel de configuração Computador e arquivos.

Como?

1. No painel esquerdo, clique no **menu Avançado**.
2. Clique em **Configurar**.
3. No painel Configurar, clique em **Computador e arquivos**.

2 Em **Proteção de SystemGuard**, clique em **Ligado**.

Observação: É possível desativar a proteção de SystemGuard clicando em **Desativar**.

Configurar opções de SystemGuards

Use o painel SystemGuards para configurar opções de proteção, registro e alerta contra alterações de arquivo e registro não autorizadas, associadas ao Internet Explorer, a programas e a arquivos do Windows. Alterações de registro e arquivo não autorizadas podem danificar seu computador, comprometer sua segurança e danificar arquivos de sistema importantes.

1. Abra o painel SystemGuards.

   Como?

   1. Em **Tarefas comuns**, clique em **Início**.
   2. No painel Início do SecurityCenter, clique em **Computador e arquivos**.
   3. Na área de informações de Computador e arquivos, clique em **Configurar**.
   4. No painel de configuração Computador e arquivos, verifique se a proteção do SystemGuard está ativada e clique em **Avançado**.

2. Selecione um tipo de SystemGuard na lista.
   - **SystemGuards de programas**
   - **SystemGuards do Windows**
   - **SystemGuards de navegador**

3. Em **Desejo**, execute uma das seguintes ações:
   - Para detectar, registrar e relatar alterações de arquivo e registro não autorizadas associadas a SystemGuards de programa, do Windows ou de navegador, clique em **Mostrar alertas.**
   - Para detectar e registrar alterações de arquivo e registro não autorizadas associadas a SystemGuards de programa, do Windows e de navegador, clique em **Registrar apenas as alterações**.
   - Para desativar a detecção de alterações de arquivo e registro não autorizadas, associadas ao SystemGuards de navegador, de programas e do Windows, clique em **Desativar o SystemGuard.**

Observação: Para obter mais informações sobre tipos de SystemGuards, consulte Sobre tipos de SystemGuards (página 49).

Sobre tipos de SystemGuards

Os SystemGuards detectam alterações potencialmente não autorizadas no registro do computador e em outros arquivos importantes que são essenciais para o Windows. Há três tipos de SystemGuards: SystemGuards de programa, SystemGuards do Windows e SystemGuards de navegador.

SystemGuards de programas

A tecnologia SystemGuards de programa pára os programas ActiveX suspeitos (baixados da Internet), além de spyware e dos programas potencialmente indesejados que podem iniciar automaticamente quando o Windows inicia.

SystemGuard	Detecta...
Instalações de ActiveX	Alterações de registro não autorizadas em instalações do ActiveX que podem danificar seu computador, comprometer sua segurança e danificar arquivos de sistema importantes.
Itens de inicialização	Spywares, adwares e outros programas potencialmente indesejados que podem instalar alterações de arquivos nos itens da Inicialização, permitindo que programas suspeitos sejam executados quando você iniciar o computador.
Ganchos de execução de shell do Windows	Spywares, adwares ou outros programas potencialmente indesejados podem instalar ganchos de execução de shell do Windows para impedir a execução adequada de programas de segurança.
Carregamento de atraso do objeto de serviço do Shell	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro no carregamento de atraso do objeto de serviço do Shell, permitindo que programas prejudiciais sejam executados quando você iniciar o computador.

SystemGuards do Windows

A tecnologia SystemGuards do Windows ajuda a impedir o computador de enviar e receber informações pessoais ou não autorizadas pela Internet. Também ajuda a bloquear programas suspeitos que trazem alterações indesejadas para a aparência e o comportamento de programas importantes para você e sua família.

SystemGuard	Detecta...
Identificadores do menu contextual	Alterações de registro não autorizadas nos identificadores de menu de contexto do Windows que podem afetar a aparência e o comportamento dos menus do Windows. Menus de contexto permitem que você execute ações em seu computador, como clicar com o botão direito do mouse em arquivos.
DLLs do AppInit	Alterações de registro não autorizadas em appInit_DLLs do Windows que podem permitir que arquivos potencialmente perigosos sejam executados quando você iniciar o computador.
Arquivo Hosts do Windows	Spywares, adwares e programas potencialmente indesejados que podem fazer alterações não autorizadas em seu arquivo hosts do Windows, permitindo que seu navegador seja redirecionado para sites da Web suspeitos e bloqueie atualizações de software.
Shell Winlogon	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro no shell Winlogon, permitindo que outros programas substituam o Windows Explorer.
Inicialização de usuário Winlogon	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro na inicialização de usuário Winlogon, permitindo que programas suspeitos sejam executados quando você efetuar logon no Windows.
Protocolos do Windows	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro nos protocolos do Windows, afetando o modo como seu computador envia e recebe informações da Internet.
Provedores de serviços em camadas Winsock	Spywares, adwares e outros programas potencialmente indesejados que podem instalar alterações de registro em Provedores de serviços em camadas (LSPs) Winsock para interceptar e alterar informações que você recebe e envia pela Internet.
Comandos abertos do Shell do Windows	Alterações não autorizadas nos comandos abertos do shell do Windows que podem permitir que worms e outros programas prejudiciais sejam executados no computador.

SystemGuard	Detecta...
Programador de tarefas compartilhada s	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro e arquivos no programador de tarefas compartilhadas, permitindo que programas potencialmente prejudiciais sejam executados quando você iniciar o computador.
Serviço do Windows Messenger	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro no serviço do Windows Messenger, permitindo anúncios não solicitados e programas executados remotamente em seu computador.
Arquivo Win.ini do Windows	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações no arquivo Win.ini, permitindo que programas suspeitos sejam executados quando você iniciar o computador.

SystemGuards de navegador

A tecnologia SystemGuards de navegador ajuda a impedir a atividade de navegador não autorizado, como redirecionamento para sites suspeitos, alterações nas configurações e opções do navegador sem seu conhecimento e confiança indesejada de sites suspeitos.

SystemGuard	Detecta...
Objetos auxiliares do navegador	Spywares, adwares e outros programas potencialmente indesejados que podem usar objetos de ajuda do navegador para rastrear a navegação na Web e exibir anúncios não solicitados.
Barras do Internet Explorer	Alterações de registro não autorizadas em programas da Barra do Internet Explorer, como Pesquisar e Favoritos, que podem afetar a aparência e o comportamento do Internet Explorer.
Extensões do Internet Explorer	Spywares, adwares e outros programas potencialmente indesejados que podem instalar extensões do Internet Explorer para rastrear a navegação na Web e exibir anúncios não solicitados.
ShellBrowser do Internet Explorer	Alterações de registro não autorizadas no navegador de shell do Internet Explorer que podem afetar a aparência e o comportamento de seu navegador da Web.
WebBrowser do Internet Explorer	Alterações de registro não autorizadas no navegador da Web do Internet Explorer que podem afetar a aparência e o comportamento de seu navegador.

SystemGuard	Detecta...
Ganchos de pesquisa de URL do Internet Explorer	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro nos ganchos de pesquisa de URL do Internet Explorer, permitindo que seu navegador seja redirecionado para sites suspeitos ao fazer pesquisas na Internet.
URLs do Internet Explorer	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro nos URLs do Internet Explorer, afetando as configurações do navegador.
Restrições do Internet Explorer	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro nas restrições do Internet Explorer, afetando as configurações e opções do navegador.
Zonas de segurança do Internet Explorer	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro nas zonas de segurança do Internet Explorer, permitindo que arquivos potencialmente prejudiciais sejam executados quando você iniciar o computador.
Sites confiáveis do Internet Explorer	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro nos sites confiáveis do Internet Explorer, permitindo que seu navegador confie em sites suspeitos.
Política do Internet Explorer	Spywares, adwares e outros programas potencialmente indesejados que podem fazer alterações de registro nas políticas do Internet Explorer, afetando a aparência e as configurações do navegador.

Usando listas confiáveis

Se o VirusScan detectar uma alteração de arquivo ou registro (SystemGuard), um programa ou uma sobrecarga do buffer, ele solicita que você confie nele ou remova-o. Se você confiar no item e indicar que não deseja receber nenhuma notificação futura sobre sua atividade, o item será adicionado a uma lista confiável e o VirusScan não o detectará mais nem o notificará sobre sua atividade. Se um item tiver sido adicionado a uma lista confiável, mas você decidir que deseja bloquear sua atividade, poderá fazer isso. O bloqueio impede o item de executar ou fazer qualquer alteração no computador sem notificá-lo sempre que você fizer uma tentativa. Também é possível remover um item de uma lista confiável. A remoção permite que o VirusScan detecte a atividade do item novamente.

Gerenciar listas confiáveis

Use o painel Listas confiáveis para confiar ou bloquear itens que foram detectados anteriormente e eram confiáveis. Também pode remover um item de uma lista confiável, de forma que o VirusScan o detecte novamente.

1 Abra o painel Listas confiáveis.

Como?

1. Em **Tarefas comuns**, clique em **Iniciar**.
2. No painel Início do SecurityCenter, clique em **Computador e arquivos**.
3. Na área de informações Computador e arquivos, clique em **Configurar**.
4. No painel de configuração Computador e arquivos, verifique se a proteção contra vírus está ativada e clique em **Avançado**.
5. Clique em **Listas confiáveis** no painel Proteção contra vírus.

2 Selecione um dos seguintes tipos de listas confiáveis:

- **SystemGuards de programas**
- **SystemGuards do Windows**
- **SystemGuards de navegador**
- **Programas confiáveis**
- **Sobrecargas de buffer confiáveis**

3 Em **Desejo**, execute uma das seguintes ações:

- Para permitir que o item detectado faça alterações no registro do Windows ou em arquivos importantes do sistema de seu computador sem notificá-lo.clique em **Confiar**.

- Para bloquear o item detectado de fazer alterações no registro do Windows ou em arquivos importantes do sistema de seu computador sem notificá-lo.clique em **Bloquear**.
- Para remover o item detectado das listas confiáveis, clique em **Remover**.

4 Clique em **OK**.

Observação: Para obter mais informações sobre tipos de listas confiáveis, consulte Sobre tipos de listas confiáveis (página 54).

Sobre tipos de listas confiáveis

Os SystemGuards no painel Listas confiáveis representam as alterações de arquivo e registro anteriormente não autorizadas que o VirusScan detectou, mas que você escolheu para permitir de um alerta ou do painel Resultados da varredura. Há cinco tipos de listas confiáveis que você pode gerenciar no painel Listas confiáveis: SystemGuards de programa, SystemGuards do Windows, SystemGuards de navegador, Programas confiáveis e Sobrecargas de buffer confiáveis.

Opção	Descrição
SystemGuards de programas	Os SystemGuards de programa no painel Listas confiáveis representam as alterações de arquivo e registro anteriormente não autorizadas que o VirusScan detectou, mas que você optou por permitiu de um alerta ou do painel Resultados da varredura. Os SystemGuards de programa detectam alterações de arquivo e registro não autorizadas associadas a instalações do ActiveX, itens de inicialização, ganchos de execução de shell do Windows e atividade de carregamento de atraso do objeto de serviço de shell. Esses tipos de alterações de registro e arquivo não autorizadas podem danificar seu computador, comprometer sua segurança e danificar arquivos de sistema importantes.

Opção	Descrição
SystemGuards do Windows	Os SystemGuards de Windows no painel Listas confiáveis representam as alterações de arquivo e registro anteriormente não autorizadas que o VirusScan detectou, mas que você optou por permitiu de um alerta ou do painel Resultados da varredura. Os SystemGuards do Windows detectam alterações de arquivo e registro não autorizadas associadas a identificadores do menu de contexto, DLLs de appInit, o arquivo hosts do Windows, o shell do Winlogon, os LSPs (Layered Service Providers) do Winsock e assim por diante. Esses tipos de alterações de arquivo e registro não autorizadas podem afetar como o computador envia e recebe informações sobre a Internet, alterar a aparência e o comportamento de programas e permitir que programas suspeitos sejam executados no computador.
SystemGuards de navegador	Os SystemGuards de navegador no painel Listas confiáveis representam as alterações de arquivo e registro anteriormente não autorizadas que o VirusScan detectou, mas que você escolheu permitir, a partir de um alerta ou do painel Resultados da varredura. Os SystemGuards de navegador detectam alterações de registro não autorizadas e outro comportamento indesejado associado a objeto de ajuda do navegador, extensões do Internet Explorer, URLs do Internet Explorer, zonas de segurança do Internet Explorer e assim por diante. Esses tipos de alterações de registro não autorizadas podem resultar em atividades de navegador indesejadas, como redirecionamento a sites suspeitos, alterações nas configurações e opções do navegador, e confiança em sites suspeitos.
Programas confiáveis	Programas confiáveis são programas potencialmente indesejados que o VirusScan detectou anteriormente, mas que foram escolhidas para serem confiáveis de um alerta ou do painel Resultados da varredura.
Sobrecargas de buffer confiáveis	Sobrecargas de buffer confiáveis representam a atividade anteriormente indesejada que o VirusScan detectou, mas que você escolheu para confiar a partir de um alerta ou do painel Resultados da varredura. Sobrecargas de buffer podem danificar seu computador e seus arquivos. Sobrecargas de buffer ocorrem quando a quantidade de informações que programas ou processos suspeitos armazenam em um buffer excedem a capacidade do buffer.

CAPÍTULO 11

Fazendo varredura no computador

Quando você iniciar o SecurityCenter pela primeira vez, a proteção antivírus em tempo real do VirusScan começa a proteger o seu computador contra vírus potencialmente mal-intencionados, cavalos de Tróia e outras ameaças de segurança. A menos que você desative a proteção antivírus em tempo real, o VirusScan monitora constantemente o computador para detectar atividades de vírus, fazendo uma varredura nos arquivos, cada vez que eles são acessados por você ou pelo computador, utilizando as opções de varredura em tempo real definidas. Para se certificar de que o computador está protegido contra as ameaças de segurança mais recentes, mantenha ativada a proteção antivírus em tempo real e configure a programação para varreduras manuais mais abrangentes. Para obter mais informações sobre a definição de opções de varredura em tempo real e manual, consulte Configurando proteção antivírus (página 39).

O VirusScan oferece um conjunto mais detalhado de opções de varredura para proteção antivírus manual, permitindo que você execute periodicamente varreduras mais abrangentes. Você pode executar varreduras a partir do SecurityCenter manualmente, orientadas a locais específicos, de acordo com uma programação definida. Contudo, também é possível executar varreduras manuais diretamente no Windows Explorer, enquanto você trabalha. A varredura no SecurityCenter oferece a vantagem de alterar as opções de varredura em tempo real. No entanto, a varredura a partir do Windows Explorer oferece uma abordagem conveniente para a segurança do computador.

Se optar por executar manualmente a varredura a partir do SecurityCenter ou do Windows Explorer, você poderá exibir seus resultados assim que ela estiver concluída. Você visualiza os resultados de uma varredura para determinar se o VirusScan detectou, reparou ou colocou em quarentena vírus, cavalos de Tróia, spyware, adware, cookies e outros programas potencialmente indesejados. Os resultados de uma varredura podem ser exibidos de formas diferentes. Por exemplo, você pode exibir um resumo básico dos resultados da varredura ou as informações detalhadas, como o status ou o tipo da infecção. Você também pode exibir estatísticas de detecção e varredura geral.

Neste capítulo

Fazer varredura no computador

Você pode executar uma varredura manual a partir do menu Avançado ou Básico do SecurityCenter. Se executar uma varredura a partir do menu Avançado, você poderá confirmar suas opções manuais antes de iniciá-la. Se você executar uma varredura a partir do menu Básico, o VirusScan iniciará a varredura imediatamente, utilizando as opções existentes. Também é possível executar uma varredura no Windows Explorer utilizando as opções de varredura existentes.

- Siga um destes procedimentos:

Fazer varredura no SecurityCenter

Para...	Faça isto...
Fazer varredura usando as configurações existentes	Clique em **Fazer varredura**, no menu Básico.
Fazer varredura usando as configurações alteradas	Clique em **Fazer varredura**, no menu Avançado, selecione os locais que serão examinados, selecione as opções de varredura e clique em **Fazer a varredura agora**.

Fazer varredura no Windows Explorer

1. Abra o Windows Explorer.
2. Clique com o botão direito no arquivo, na pasta ou no disco rígido e clique em **Fazer varredura**.

Observação: Os resultados da varredura são exibidos no alerta de Varredura concluída. Os resultados incluem o número de itens examinados, detectados, colocados em quarentena e removidos. Clique em **Exibir detalhes da varredura** para saber mais sobre os resultados da varredura ou sobre como trabalhar com itens infectados.

Exibir resultados da varredura

Quando uma varredura manual for concluída, você visualizará os resultados para determinar o que a varredura detectou e para analisar o status de proteção atual do computador. Os resultados da varredura indicam se o VirusScan detectou, reparou ou colocou em quarentena vírus, cavalos de Tróia, spyware, adware, cookies e outros programas potencialmente indesejados.

- No menu Básico ou Avançado, clique em **Fazer varredura** e em seguida execute um dos procedimentos a seguir:

Para...	Faça isto...
Exibir os resultados da varredura no alerta	Exibir os resultados da varredura no alerta de Varredura concluída.
Exibir mais informações sobre os resultados da varredura	Clique em **Exibir detalhes da varredura** no alerta de Varredura concluída.
Exibir um resumo rápido dos resultados da varredura	Aponte para o **ícone de Varredura concluída**, na área de notificação da barra de tarefas.
Exibir a estatística de detecção e varredura	Aponte para o ícone de **Varredura concluída** na área de notificação da barra de tarefas.
Exibir os detalhes sobre os itens detectados e o status e o tipo da infecção.	Clique duas vezes no ícone de **Varredura concluída**, na área de notificação da barra de tarefas e, em seguida, clique em **Exibir resultados**, no Andamento da varredura: painel Varredura manual.

CAPÍTULO 12

Trabalhando com resultados da varredura

Se o VirusScan detectar uma ameaça à segurança, enquanto estiver executando uma varredura em tempo real ou manual, ele tentará conter a ameaça automaticamente, dependendo do tipo da ameaça. Por exemplo, se o VirusScan detectar um vírus, cavalo de Tróia ou cookie de rastreamento no computador, ele tentará limpar o arquivo infectado. Se não conseguir, ele colocará o arquivo em quarentena.

Com algumas ameaças de segurança, o VirusScan pode não conseguir limpar ou colocar o arquivo em quarentena. Nesse caso, o VirusScan solicita que você lide com a ameaça. Há várias formas de agir, dependendo do tipo de ameaça. Por exemplo, se um vírus for detectado em um arquivo, mas o VirusScan não for capaz de limpá-lo ou colocá-lo em quarentena, o acesso ao arquivo será negado. Se cookies de rastreamento forem detectados, mas o VirusScan não for capaz de limpar ou colocar os cookies em quarentena, você poderá optar por removê-los ou confiar neles. Se programas potencialmente indesejados forem detectados, o VirusScan não realizará nenhuma ação automaticamente, ele permitirá que você decida se deseja confiar no programa ou colocá-lo em quarentena.

Quando o VirusScan coloca itens em quarentena, ele criptografa e depois isola os itens em uma pasta para evitar que arquivos, programas e cookies danifiquem o seu computador. Você pode restaurar ou remover os itens em quarentena. Na maioria dos casos, você pode excluir um cookie em quarentena sem afetar o sistema. Contudo, se o VirusScan tiver colocado em quarentena um programa que você reconheça e utilize, é recomendável restaurá-lo.

Neste capítulo

Trabalhar com vírus e cavalos de Tróia

Se o VirusScan detectar um vírus ou um cavalo de Tróia em um arquivo no computador durante uma varredura em tempo real ou manual, ele tentará limpar o arquivo. Se não conseguir, o ele tentará colocar o arquivo em quarentena. Se essa operação também falhar, o acesso aos arquivos será negado (somente em varreduras em tempo real).

1 Abrir o painel Resultados da varredura.

Como?

1. Aponte para o ícone de **Varredura concluída** na área de notificação à direita da barra de tarefas.
2. No Andamento da varredura: No painel Varredura manual, clique em **Exibir resultados**.

2 Na lista de resultados da varredura, clique em **Vírus e cavalos de Tróia**.

Observação: Para trabalhar com os arquivos que o VirusScan colocou em quarentena, consulte Trabalhar com arquivos em quarentena (página 63).

Trabalhar com programas potencialmente indesejáveis

Se o VirusScan detectar um programa potencialmente indesejado no computador durante uma varredura em tempo real ou manual, você poderá confiar no programa ou removê-lo. Remover o programa potencialmente indesejado não o exclui do sistema. Na verdade, a remoção coloca o programa em quarentena para evitar que ele danifique os arquivos do computador.

1 Abrir o painel Resultados da varredura.

Como?

1. Aponte para o ícone de **Varredura concluída** na área de notificação à direita da barra de tarefas.
2. No Andamento da varredura: No painel Varredura manual, clique em **Exibir resultados**.

2 Na lista de resultados da varredura, clique em **Programas potencialmente indesejados**.

3 Selecione um programa potencialmente indesejado.

4 Em **Desejo**, clique em **Remover** ou **Confiar**.

5 Confirme a opção que você selecionou.

Trabalhar com arquivos em quarentena

Quando o VirusScan coloca arquivos em quarentena, ele criptografa e envia os arquivos para uma pasta, para evitar que eles danifiquem o computador. Você pode restaurar ou remover os arquivos em quarentena.

1 Abrir o painel Arquivos em quarentena.

Como?

1. No painel esquerdo, clique no **Menu avançado**.
2. Clique em **Restaurar**.
3. Clique em **Arquivos**.

2 Selecione um arquivo em quarentena.

3 Siga um destes procedimentos:

- Para reparar o arquivo infectado e devolvê-lo ao local em que estava armazenado em seu computador, clique em **Restaurar**.
- Para remover o arquivo infectado do seu computador, clique em **Remover**.

4 Clique em **Sim** para confirmar a opção que você selecionou.

Dica: Você pode restaurar ou remover vários arquivos ao mesmo tempo.

Trabalhar com cookies e programas em quarentena

Quando o VirusScan coloca em quarentena programas potencialmente indesejados ou cookies de rastreamento, ele os criptografa e depois os envia para uma pasta protegida, para evitar que eles danifiquem o computador. Então, você poderá restaurar ou remover os itens em quarentena. Na maioria dos casos, você pode excluir um item em quarentena sem afetar o sistema.

1 Abrir o painel Programas em quarentena e cookies de rastreamento.

Como?

1. No painel esquerdo, clique no **Menu avançado**.
2. Clique em **Restaurar**.
3. Clique em **Programas e cookies**.

2 Selecione um cookie ou programa em quarentena.

3 Siga um destes procedimentos:

- Para reparar o arquivo infectado e devolvê-lo ao local em que estava armazenado em seu computador, clique em **Restaurar**.
- Para remover o arquivo infectado do seu computador, clique em **Remover**.

4 Clique em **Sim** para confirmar a operação.

Dica: Você pode restaurar ou remover vários programas e cookies ao mesmo tempo.

CAPÍTULO 13

McAfee Personal Firewall

O Personal Firewall oferece proteção avançada para seu computador e seus dados pessoais. O Personal Firewall estabelece uma barreira entre o seu computador e a Internet, monitorando de forma silenciosa o tráfego da Internet em busca de atividades suspeitas.

Observação: O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician.

Neste capítulo

Recursos do Personal Firewall

O Personal Firewall fornece os seguintes recursos.

Níveis de proteção padrão e personalizado

Proteção contra invasões e atividades suspeitas utilizando as configurações de proteção personalizáveis ou padrão do Firewall.

Recomendações em tempo real

Receba recomendações de forma dinâmica para ajudá-lo a determinar se os programas devem ter acesso à Internet ou se o tráfego de rede é confiável.

Gerenciamento inteligente de acesso para programas

Gerencie o acesso à Internet para programas, através de alertas e registros de eventos, e configure permissões de acesso para programas específicos

Proteção para jogos

Evite que os alertas relativos a tentativas de invasão e atividades suspeitas o distraiam enquanto você joga em tela cheia.

Proteção de inicialização do computador

Assim que o ?Windows® é iniciado, o Firewall protege o computador contra tentativas de invasão, programas indesejados e tráfego de rede.

Controle da porta de serviço do sistema

Gerencie portas de serviço do sistema abertas e fechadas exigidas por alguns programas.

Gerenciamento de conexões do computador

Permita e bloqueie conexões remotas entre o seu computador e outros computadores.

Integração com informações do HackerWatch

Rastreie padrões de invasão e hackers globais através do site do HackerWatch, que também fornece informações de segurança atuais sobre programas de seu computador, bem como eventos de segurança globais e estatísticas de portas de Internet.

Firewall bloqueado

Bloqueie instantaneamente todo o tráfego de entrada e de saída entre o computador e a Internet.

Restauração do Firewall

Restaure instantaneamente as configurações originais de proteção do Firewall.

Detecção avançada de Cavalos de Tróia

Detecte e bloqueie aplicativos potencialmente mal-intencionados, como cavalos de Tróia, impedindo que seus dados pessoais sejam transmitidos pela Internet.

Registro de eventos

Rastreie eventos de invasão, entrada e saída recentes.

Monitoramento do tráfego de Internet

Analise mapas mundiais que mostram a origem de ataques e tráfego hostis. Além disso, localize informações detalhadas sobre o proprietário e dados geográficos de endereços IP de origem. Analise também o tráfego de entrada e saída, monitore a largura de banda e as atividades dos programas.

Prevenção de invasões

Proteja a sua privacidade contra possíveis ameaças da Internet. Utilizando a funcionalidade heurística, a McAfee fornece uma terceira camada de proteção, através do bloqueio de itens que exibem sintomas de ataques ou características de atividades de hackers.

Análise sofisticada de tráfego

Analise o tráfego de entrada e saída de Internet e as conexões de programas, inclusive aquelas que estão ouvindo ativamente as conexões abertas. Isso permite que você veja e tome providências em relação a programas que possam estar vulneráveis a invasões.

CAPÍTULO 14

Iniciando o Firewall

Assim que você instalar o Firewall, seu computador estará protegido contra invasões e tráfego de rede indesejado. Além disso, você estará pronto para lidar com alertas e gerenciar o acesso de entrada e saída da Internet para programas conhecidos e desconhecidos. Recomendações inteligentes e nível de segurança Confiável (com a opção para permitir somente acesso de saída de um programa à Internet selecionada) são ativados automaticamente.

Você pode desativar o Firewall no painel Internet & Configuração de rede, mas seu computador não estará mais protegido contra invasões e tráfego de rede indesejado, e você não poderá gerenciar eficientemente as conexões de entrada e saída com a Internet. Se você precisar desativar a proteção de firewall, faça-o temporariamente e apenas quando necessário. Você também pode ativar o Firewall a partir do painel Internet & Configuração de rede.

O Firewall desativa automaticamente o Windows® Firewall e se define como o firewall padrão.

Observação: Para configurar o Firewall, abra o painel Configuração de rede e Internet.

Neste capítulo

Iniciar proteção de firewall

É possível ativar o Firewall para proteger seu computador contra invasões e tráfego de rede indesejado, além de gerenciar as conexões de entrada e de saída da Internet.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e, em seguida, clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall está desativada**, clique em **Ativar**.

Interromper proteção de firewall

Você pode desativar seu Firewall se não desejar proteger seu computador contra invasões e tráfego de rede indesejado. Quando o Firewall está desativado, não é possível gerenciar conexões de Internet de entrada e saída.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall está ativada**, clique em **Desativar**.

CAPÍTULO 15

Trabalhando com alertas

O Firewall utiliza uma gama de alertas para ajudá-lo a gerenciar sua segurança. Esses alertas podem ser agrupados em três tipos básicos:

- Alerta vermelho
- Alerta amarelo
- Alerta verde

Os alertas também podem conter informações para ajudá-lo a decidir como lidar com alertas ou obter informações sobre os programas em execução no computador.

Neste capítulo

Sobre alertas

O Firewall tem três tipos básicos de alertas. Alguns desses alertas incluem informações para ajudá-lo a obter informações sobre programas executados em seu computador.

Alerta vermelho

O alerta vermelho aparece quando o Firewall detecta e bloqueia um cavalo de Tróia no computador, e recomenda que você faça uma varredura para buscar outras ameaças. Um Cavalo de Tróia parece ser um programa legítimo, mas pode atrapalhar, danificar ou fornecer acesso não autorizado ao seu computador. Este alerta ocorre em todos os níveis de segurança, exceto no Aberto.

Alerta amarelo

O tipo de alerta mais comum é o amarelo, que informa você sobre a atividade de um programa ou evento de rede detectado pelo Firewall. Quando isso ocorre, o alerta descreve a atividade do programa ou o evento de rede e apresenta uma ou mais opções que exigem uma resposta sua. Por exemplo, o alerta **Nova rede detectada** é exibido quando um computador com Firewall instalado é conectado a uma nova rede. Você pode escolher confiar ou não confiar na rede. Se a rede for confiável, o Firewall permite o tráfego a partir de qualquer outro computador da rede e a adiciona aos Endereços IP confiáveis. Se as Recomendações inteligentes estiverem ativadas, os programas serão adicionados ao painel Permissões do programa.

Alerta verde

Na maioria dos casos, um alerta verde fornece informações básicas sobre um evento e não requer uma resposta. Alertas verdes são desabilitados por padrão e normalmente ocorrem quando os níveis de segurança Padrão, Confiável, Rígido e Oculto estão definidos.

Assistência ao usuário

Muitos alertas do firewall contêm informações adicionais para ajudá-lo a gerenciar a segurança do computador. Entre elas estão as seguintes:

- **Saiba mais sobre este programa**: Acessar o site de segurança global da McAfee na Web para obter informações sobre um programa detectado pelo Firewall em seu computador.
- **Informe a McAfee sobre este programa**: Enviar informações à McAfee sobre um arquivo desconhecido que o firewall detectou em seu computador.

- **A McAfee recomenda**: Informações sobre o gerenciamento de alertas. Por exemplo, um alerta pode recomendar que você permita acesso a um programa.

CAPÍTULO 16

Gerenciando alertas informativos

O Firewall permite que você exiba ou oculte alertas informativos quando detecta tentativas de invasão ou atividades suspeitas durante determinados eventos, por exemplo, durante um jogo em tela cheia.

Neste capítulo

Exibir alertas durante jogos

Você pode permitir que alertas informativos do Firewall sejam exibidos quando detectar tentativas de invasão ou atividades suspeitas durante um jogo em tela cheia.

1. No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2. Clique em **Configurar**.
3. No painel Configuração do SecurityCenter, em **Alertas**, clique em **Avançado**.
4. No painel Opções de alerta, selecione **Mostrar alertas informativos quando o modo de jogo for detectado**.
5. Clique em **OK**.

Ocultar alertas informativos

Você pode evitar que alertas informativos do Firewall sejam exibidos quando ele detectar tentativas de invasão ou atividades suspeitas.

1. No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2. Clique em **Configurar**.
3. No painel Configuração do SecurityCenter, em **Alertas**, clique em **Avançado**.
4. No painel Configuração do SecurityCenter, clique em **Alertas informativos**.
5. No painel Alertas informativos, execute um dos procedimentos a seguir:
   - Selecione **Não mostrar alertas informativos** para ocultar todos os alertas informativos.
   - Desmarque um alerta para ocultar.
6. Clique em **OK**.

CAPÍTULO 17

Configurando a proteção do Firewall

O Firewall oferece vários métodos para gerenciar sua segurança e personalizar a maneira como você deseja responder a eventos e alertas de segurança.

Depois que você instalar o Firewall pela primeira vez, o nível de segurança de proteção do seu computador será definido como Confiável e seus programas só terão acesso de saída à Internet. No entanto, o Firewall oferece outros níveis, que vão do altamente restritivo ao altamente permissivo.

O Firewall também oferece a oportunidade de receber recomendações sobre alertas e acesso de programas à Internet.

Neste capítulo

Gerenciando os níveis de segurança do Firewall

Os níveis de segurança do Firewall controlam em que nível que você deseja gerenciar e responder alertas. Esses alertas são exibidos quando o firewall detecta tráfego de rede e conexões de entrada e saída de Internet indesejados. Por padrão, o nível de segurança do Firewall é definido como Confiável, com acesso de saída apenas.

Quando o nível de segurança Confiável está definido e as Recomendações inteligentes estão ativadas, alertas amarelos fornecem a opção de permitir ou bloquear o acesso de programas desconhecidos que exigem acesso de entrada. Quando programas conhecidos são detectados, são exibidos alertas informativos verdes e o acesso é permitido automaticamente. A concessão de acesso permite que um programa crie conexões de saída e escute as conexões de entrada não solicitadas.

Geralmente, quanto mais restritivo for o nível de segurança (Oculto e Rígido), maior será o número de opções e alertas exibidos com os quais você precisará lidar.

A tabela a seguir descreve os seis níveis de segurança do Firewall, começando pelo mais restritivo até o menos restritivo:

Nível	Descrição
Bloqueado	Bloqueia todas as conexões de rede de entrada e de saída, incluindo o acesso a sites da Web, e-mails e atualizações de segurança. Este nível de segurança tem o mesmo resultado que a remoção de sua conexão com a Internet. Use esta configuração para bloquear as portas definidas como abertas no painel Serviços do sistema.
Oculto	Bloqueia todas as conexões de Internet de entrada, exceto portas abertas, ocultando a presença de seu computador na Internet. O firewall avisa você quando novos programas tentam estabelecer conexões de saída com a Internet ou recebem solicitações de conexão de entrada. Os programas bloqueados e adicionados aparecem no painel Permissões do programa.
Rígida	Alerta você quando novos programas tentam estabelecer conexões de saída com a Internet ou recebem solicitações de conexão de entrada. Os programas bloqueados e adicionados aparecem no painel Permissões do programa. Quando o nível de segurança é definido como Rígido, o programa solicita apenas o tipo de acesso exigido naquele momento, por exemplo, acesso apenas de saída, que você pode permitir ou bloquear. Mais tarde, se o programa exigir uma conexão de saída e também de entrada, você poderá conceder acesso total no painel Permissões do programa.

Nível	Descrição
Padrão	Monitora conexões de entrada e de saída e avisa quando novos programas tentam acessar a Internet. Os programas bloqueados e adicionados aparecem no painel Permissões do programa.
Confiável	Permite que programas tenham acesso de entrada e saída (total) ou somente acesso de saída à Internet. O nível de segurança padrão é Confiável, com a opção selecionada para permitir somente acesso de saída para programas. Se um programa tiver acesso total, o Firewall confiará automaticamente nele e o adicionará à lista de programas permitidos no painel Permissões do programa. Se um programa tiver somente acesso de saída, então o Firewall confiará automaticamente nele ao realizar uma conexão somente de saída à Internet. Uma conexão de entrada não é automaticamente confiável.
aberta	Permite todas as conexões de entrada e saída com a Internet.

O Firewall também permite que você redefina imediatamente seu nível de segurança como Confiável (e permita acesso somente de saída) no painel Restaurar padrões de proteção do Firewall.

Definir nível de segurança como Bloqueado

Você pode definir o nível de segurança do Firewall para Bloqueado para bloquear todas as conexões de rede de entrada e saída.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall está ativada**, clique em **Avançado**.
3. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Bloqueado**.
4. Clique em **OK**.

Definir nível de segurança como Oculto

É possível definir o nível de segurança do Firewall para Oculto para bloquear todas as conexões de rede de entrada, exceto portas abertas, para ocultar a presença de seu computador na Internet.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall está ativada**, clique em **Avançado**.
3. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Oculto**.
4. Clique em **OK**.

Observação: No modo Oculto, o Firewall avisa você quando novos programas solicitam conexão de saída à Internet ou recebem solicitações de conexão de entrada.

Definir nível de segurança como Rígido

É possível definir o nível de segurança do Firewall como Rígido para receber alertas quando novos programas tentarem estabelecer conexões de saída com a Internet ou receberem solicitações de conexão de entrada.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall está ativada**, clique em **Avançado**.
3. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Rígido**.
4. Clique em **OK**.

Observação: No modo Rígido, um programa solicita apenas o tipo de acesso exigido naquele momento, por exemplo, acesso apenas de saída, que você pode permitir ou bloquear. Mais tarde, se o programa exigir tanto uma conexão de saída como uma de entrada, você poderá conceder acesso total ao programa no painel Permissões do programa.

Definir nível de segurança como Padrão

É possível definir o nível de segurança como Padrão para monitorar conexões de entrada e de saída, e alertar você quando novos programas tentarem acessar a Internet.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e, em seguida, clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall está ativada**, clique em **Avançado**.
3. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Padrão**.
4. Clique em **OK**.

Definir nível de segurança como Confiável

Você pode definir o nível de segurança do Firewall como Confiável para permitir acesso total ou somente acesso de saída à rede.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Confiável**.
4. Siga um destes procedimentos:
   - Para permitir acesso total à rede de entrada e de saída, selecione **Permitir acesso total**.
   - Para permitir somente acesso de saída à rede, selecione **Permitir somente acesso de saída**.
5. Clique em **OK**.

Observação: A opção padrão é **Permitir somente acesso de saída**.

Definir nível de segurança como Aberto

É possível definir o nível de segurança do Firewall como Aberto para permitir todas as conexões de rede de entrada e de saída.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Nível de segurança, mova o botão deslizante até que o nível atual exibido seja **Aberto**.
4. Clique em **OK**.

Configurando as Recomendações inteligentes para alertas

Você pode configurar o Firewall para incluir, excluir ou exibir recomendações em alertas quando qualquer programa tentar acessar a Internet. A ativação das recomendações inteligentes ajuda você a decidir como lidar com alertas.

Quando as Recomendações inteligentes estão ativadas (e o nível de segurança está definido como Confiável com o acesso somente de saída ativado), o Firewall permite ou bloqueia programas conhecidos de forma automática e exibe no alerta uma recomendação ao detectar programas potencialmente perigosos.

Quando as Recomendações inteligentes estão desativadas, o Firewall não permite ou bloqueia o acesso à Internet, nem recomenda um plano de ação no alerta.

Quando as Recomendações inteligentes estão definidas como Somente exibir, um alerta avisa você se o acesso deve ser permitido ou bloqueado e recomenda um plano de ação.

Ativar Recomendações inteligentes

Você pode ativar as Recomendações inteligentes para o Firewall permitir ou bloquear programas automaticamente e alertar você sobre programas não reconhecidos ou potencialmente perigosos.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Nível de segurança, em **Recomendações inteligentes**, selecione **Ativar Recomendações inteligentes**.
4. Clique em **OK**.

Desativar Recomendações inteligentes

Você pode desativar as Recomendações inteligentes para o Firewall permitir ou bloquear programas e alertar você sobre programas não reconhecidos ou potencialmente perigosos. Entretanto, os alertas excluem todas as recomendações sobre o tratamento do acesso a programas. Se o Firewall detectar um novo programa suspeito ou conhecido como uma possível ameaça, ele bloqueará automaticamente o acesso do programa à Internet.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Nível de segurança, em **Recomendações inteligentes**, selecione **Desativar Recomendações inteligentes**.
4. Clique em **OK**.

Somente exibir as recomendações inteligentes

É possível exibir as Recomendações inteligentes para que os alertas forneçam somente recomendações de plano de ações para que você decida se permite ou bloqueia programas não reconhecidos ou potencialmente perigosos.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Nível de segurança, em **Recomendações inteligentes**, selecione **Somente exibir**.
4. Clique em **OK**.

Otimizando a segurança do Firewall

Há muitas maneiras pelas quais a segurança de seu computador pode ser comprometida. Por exemplo, alguns programas podem tentar se conectar à Internet antes que o Windows® seja iniciado. Além disso, usuários sofisticados podem rastrear (ou executar ping) em seu computador para verificar se ele está conectado a uma rede. O Firewall permite que você se defenda contra esses dois tipos de invasão, permitindo que você ative a proteção de inicialização e bloqueie solicitações de ping. A primeira configuração bloqueia o acesso de programas à Internet enquanto o Windows é iniciado, e a segunda bloqueia solicitações de ping que ajudam outros usuários a detectar seu computador em uma rede.

As configurações de instalação padrão incluem detecção automática para as tentativas mais comuns de invasão, como ataques de Negação de serviço ou explorações. O uso das configurações de instalação padrão garante a sua proteção contra ataques e varreduras. Entretanto, é possível desativar a detecção automática para um ou mais ataques ou procuras no painel de Detecção de intrusão.

Proteja seu computador durante a inicialização

Você pode proteger o seu computador enquanto o Windows é iniciado para bloquear novos programas que não tinham acesso à Internet (e agora precisam) durante a inicialização. O Firewall exibe alertas relevantes para programas que solicitaram acesso à Internet, e que você pode permitir ou bloquear. Para utilizar essa opção, seu nível de segurança não pode estar definido como Aberto ou Bloqueado.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Nível de segurança, em **Configurações de segurança**, selecione **Ativar proteção de inicialização**.
4. Clique em **OK**.

Observação: As conexões e invasões bloqueadas não são registradas enquanto a proteção de inicialização está ativada.

Configurações de solicitações de ping

Você pode permitir ou impedir a detecção do computador na rede por outros usuários.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Nível de segurança, em **Configurações de segurança**, execute um dos procedimentos a seguir:
   - Selecione **Permitir solicitações de ping ICMP** para permitir que seu computador seja detectado na rede por solicitações de ping.
   - Desmarque **Permitir solicitações de ping ICMP** para impedir que seu computador seja detectado na rede por solicitações de ping.
4 Clique em **OK**.

Configurar detecção de invasão

Você pode detectar tentativas de invasão para proteger seu computador contra ataques e varreduras não autorizadas. As configurações de Firewall padrão incluem a detecção automática das tentativas das invasão mais comuns, como ataques de Negação de serviço ou explorações, entretanto, você pode desativar a detecção automática de um ou mais ataques ou varreduras.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **Detecção de invasão**.
4 Em **Detectar tentativas de invasão**, escolha uma das seguintes opções:
   - Selecione um nome para fazer varredura ou detectar automaticamente o ataque.
   - Desmarque um nome para desativar a varredura ou detecção automática de ataque.
5 Clique em **OK.**

Configurar definições do Status de proteção do Firewall

Você pode configurar o Firewall para ignorar que problemas específicos em seu computador não sejam relatados no SecurityCenter.

1 No painel do McAfee SecurityCenter, em **Informações do SecurityCenter**, clique em **Configurar**.
2 No painel Configuração do SecurityCenter, em **Status de proteção**, clique em **Avançado**.
3 No painel Problemas ignorados, selecione uma ou mais das seguintes opções:
   - **Proteção de firewall desativada.**
   - **O nível de segurança do firewall está definido como Aberto.**
   - **O serviço de firewall não está sendo executado.**
   - **A Proteção de firewall não está instalada em seu computador.**
   - **Seu Firewall do Windows está desativado.**
   - **O Firewall de saída não está instalado em seu computador.**
4 Clique em **OK**.

Bloqueando e restaurando o Firewall

O recurso Bloqueado bloqueia todo o tráfego de entrada e de saída da rede para ajudar você a isolar e solucionar um problema em seu computador.

Bloquear o Firewall instantaneamente

Você pode ativar o Firewall para bloquear instantaneamente todo o tráfego de entrada e saída entre o computador e a Internet.

1 No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique em **Bloquear Firewall**.
2 No painel Bloquear Firewall, clique em **Bloquear**.
3 Clique em **Sim** para confirmar.

Dica: Você também pode bloquear o Firewall clicando com o botão direito do mouse no ícone do SecurityCenter na área de notificação à direta da barra de tarefas e, em seguida, clicando em **Links rápidos** e em **Bloquear Firewall**.

Desbloquear o Firewall instantaneamente

Você pode desativar o Firewall para permitir instantaneamente todo o tráfego de entrada e saída entre o computador e a Internet.

1 No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique em **Bloquear Firewall**.
2 No painel Bloquear Firewall, clique em **Desbloquear**.
3 Clique em **Sim** para confirmar.

Restaurar configurações do Firewall

Você pode restaurar rapidamente o Firewall para suas configurações de proteção originais. Essa restauração redefine o nível de segurança como Confiável e permite somente acesso de saída à rede, ativa as Recomendações inteligentes, restaura a lista de programas padrão e suas permissões no painel Permissões do programa, remove endereços IP confiáveis e proibidos e restaura serviços do sistema, configurações de registro de eventos e detecção de invasões.

1. No painel do McAfee SecurityCenter, clique em **Restaurar padrões do Firewall**.
2. No painel Restaurar padrões do Firewall, clique em **Restaurar padrões**.
3. Clique em **Sim** para confirmar.

Dica: Também é possível restaurar as configurações padrão do Firewall clicando com o botão direito do mouse no ícone do SecurityCenter na área de notificação à direita da barra de tarefas e, em seguida, clicando em **Links rápidos** e em **Restaurar padrões do Firewall**.

CAPÍTULO 18

Gerenciando programas e permissões

O Firewall permite que você gerencie e crie permissões de acesso para programas existentes e novos que solicitam acesso de entrada e saída à Internet. O Firewall permite que você controle o acesso total ou apenas de saída dos programas. Também é possível bloquear o acesso a programas.

Neste capítulo

Permitindo acesso de programas à Internet

Alguns programas, como navegadores de Internet, precisam acessar a Internet para funcionarem corretamente.

O Firewall permite que você use a página de Permissões do programa para:

- Permitir acesso de programas
- Permitir somente acesso de saída a programas
- Bloquear o acesso de programas

Você também pode permitir que um programa tenha acesso total e apenas de saída à Internet no registro de Eventos recentes e de Eventos de saída.

Permitir acesso total a um programa

Você pode permitir que um programa bloqueado em seu computador tenha acesso total e de saída à Internet.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **Permissões do programa**.
4. Em **Permissões do programa**, selecione um programa com acesso **Bloqueado** ou **Somente acesso de saída**.
5. Em **Ação**, clique em **Permitir acesso**.
6. Clique em **OK**.

Permitir acesso total a um programa novo

Você pode permitir que um novo programa em seu computador tenha acesso total e de saída à Internet.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **Permissões do programa**.
4. Em **Permissões do programa**, clique em **Adicionar programa permitido**.
5. Na caixa de diálogo **Adicionar programa**, procure e selecione o programa que deseja adicionar e, em seguida, clique em **Abrir**.

Observação: Você pode mudar as permissões para um novo programa adicionado do mesmo modo que para um programa existente, selecionando o programa e, em seguida, clicando em **Permitir acesso somente de saída** ou **Bloquear acesso** em **Ação**.

Permitir acesso total a partir do registro de Eventos recentes

Você pode permitir que um programa bloqueado que apareça no registro de Eventos recentes tenha acesso total e acesso de saída à Internet.

1. No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2. Clique em **Relatórios e registros**.
3. Em **Eventos recentes**, selecione a descrição do evento e clique em **Permitir acesso**.
4. Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar.

Tópicos relacionados

- Exibir eventos de saída (página 115)

Permitir acesso total a partir do registro de Eventos de saída

Você pode permitir que um programa bloqueado que apareça no registro de Eventos de saída tenha acesso total e acesso de saída à Internet.

1 No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2 Clique em **Relatórios e registros**.
3 Em **Eventos recentes**, clique em **Exibir registro**.
4 Clique em **Rede e Internet** e em **Eventos de saída**.
5 Selecione um programa e, em **Desejo**, clique em **Permitir acesso**.
6 Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar.

Permitindo somente acesso de saída a programas

Alguns programas no computador exigem acesso de saída à Internet. O Firewall permite que você configure permissões de programas para permitir somente o acesso de saída à Internet.

Permitir somente acesso de saída a um programa

Você pode permitir que um programa tenha somente acesso de saída à Internet.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **Permissões do programa**.
4. Em **Permissões do programa**, selecione um programa com acesso **Bloqueado** ou **Acesso total**.
5. Em **Ação**, clique em **Permitir somente acesso de saída**.
6. Clique em **OK**.

Permitir somente acesso de saída a partir do registro de Eventos recentes

Você pode permitir que um programa bloqueado que aparece no registro de Eventos recentes tenha acesso somente de saída à Internet.

1. No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2. Clique em **Relatórios e registros**.
3. Em **Eventos recentes**, selecione a descrição do evento e clique em **Permitir somente acesso de saída**.
4. Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar.

Permitir somente acesso de saída a partir do registro de Eventos de saída

Você pode permitir que um programa bloqueado que aparece no registro de Eventos de saída tenha acesso somente de saída à Internet.

1. No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2. Clique em **Relatórios e registros**.
3. Em **Eventos recentes**, clique em **Exibir registro**.
4. Clique em **Rede e Internet** e em **Eventos de saída**.
5. Selecione um programa e, em **Desejo**, clique em **Permitir somente acesso de saída**.
6. Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar.

Bloqueando o acesso de programas à Internet

O Firewall permite que você bloqueie o acesso de programas à Internet. Certifique-se de que o bloqueio de um programa não interromperá sua conexão de rede ou algum outro programa que exija acesso à Internet para funcionar adequadamente.

Bloquear o acesso de um programa

Você pode bloquear o acesso à Internet de entrada e de saída de um programa.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **Permissões do programa**.
4 Em **Permissões do programa**, selecione um programa com **Acesso total** ou **Somente acesso de saída**.
5 Em **Ação**, clique em **Bloquear acesso**.
6 Clique em **OK**.

Bloquear o acesso de um novo programa

Você pode bloquear o acesso à Internet de entrada e de saída de um novo programa.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **Permissões do programa**.
4 Em **Permissões do programa**, clique em **Adicionar programa bloqueado**.
5 Na caixa de diálogo Adicionar programa procure e selecione o programa que deseja adicionar e, em seguida, clique em **Abrir**.

Observação: Você pode mudar as permissões de um novo programa adicionado recentemente, selecionando o programa e, em seguida, clicando em **Permitir acesso somente de saída** ou **Permitir acesso** em **Ação**.

Bloquear o acesso a partir do registro de Eventos recentes

Você pode impedir que um programa que aparece no registro de Eventos recentes tenha acesso à Internet de entrada e de saída.

1. No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2. Clique em **Relatórios e registros**.
3. Em **Eventos recentes**, selecione a descrição do evento e clique em **Bloquear acesso**.
4. Na caixa de diálogo Permissões do programa, clique em **Sim** para confirmar.

Removendo permissões de acesso para programas

Antes de remover uma permissão de programa, verifique se a ausência dessa permissão não afeta a funcionalidade de seu computador ou a sua conexão de rede.

Remover uma permissão de programa

Você pode remover todo acesso à Internet de entrada e de saída de um programa.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **Permissões do programa**.
4 Em **Permissões do programa**, selecione um programa.
5 Em **Ação**, clique em **Remover permissões do programa**.
6 Clique em **OK**.

Observação: O Firewall impede que você modifique alguns programas, minimizando ou desativando algumas ações.

Aprendendo sobre programas

Caso não tenha certeza sobre quais permissões de programa aplicar, você poderá obter informações sobre o programa no site HackerWatch da McAfee.

Obter informações sobre programas

É possível obter informações sobre programas no site HackerWatch da McAfee para decidir se o acesso à Internet de entrada e de saída deve ser permitido ou bloqueado.

Observação: Verifique se você está conectado à Internet para que seu navegador inicie o site HackerWatch da McAfee, que fornece informações atualizadas sobre programas, solicitações de acesso à Internet e ameaças à segurança.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **Permissões do programa**.
4. Em **Permissões do programa**, selecione um programa.
5. Em **Ação**, clique em **Saiba mais**.

Obter informações do programa a partir do registro de Eventos de saída

No registro de Eventos de saída, é possível obter informações sobre programas no site HackerWatch da McAfee para decidir que programas devem ter o acesso à Internet de entrada e de saída permitido ou bloqueado.

Observação: Verifique se você está conectado à Internet para que seu navegador inicie o site HackerWatch da McAfee, que fornece informações atualizadas sobre programas, solicitações de acesso à Internet e ameaças à segurança.

1. No painel do McAfee SecurityCenter, clique em **Menu avançado**.
2. Clique em **Relatórios e registros**.
3. Em Eventos recentes, selecione um evento e clique em **Exibir registro**.
4. Clique em **Rede e Internet** e em **Eventos de saída**.
5. Selecione um endereço IP e clique em **Saiba mais**.

CAPÍTULO 19

Gerenciando os serviços do sistema:

Para funcionar corretamente, certos programas (como servidores da Web ou programas de servidor de compartilhamento de arquivos) precisam aceitar conexões não solicitadas de outros computadores através de portas de serviço de sistema designadas. Tipicamente, o Firewall fecha essas portas de serviço do sistema, porque eles representam as fontes mais prováveis de insegurança do sistema. Para aceitar conexões de computadores remotos, no entanto, as portas de serviço do sistema devem ser abertas.

Neste capítulo

Configurando portas de serviço do sistema

Portas de serviço do sistema podem ser configuradas para permitir ou bloquear acesso de rede remoto a um serviço no computador.

A lista abaixo mostra os serviços de sistema comuns e as portas associadas:

- Portas 20-21 do FTP (Protocolo de Transferência de Arquivos)
- Porta 143 do servidor de e-mail (IMAP)
- Porta 110 do servidor de e-mail (POP3)
- Porta 25 do servidor de e-mail (SMTP)
- Porta 445 do Microsoft Directory Server (MSFT DS)
- Porta 1433 do Microsoft SQL Server (MSFT SQL)
- Porta 123 NTP (Network Time Protocol)
- Área de trabalho remota / Assistência remota / Servidor de Terminal (RDP) Porta 3389
- Chamadas de procedimento remoto (RPC) Porta 135
- Porta 443 do servidor Web seguro (HTTPS)
- Porta 5000 de Plug and Play Universal (UPNP)
- Porta 80 do servidor Web (HTTP)
- Portas 137-139 do compartilhamento de arquivos do Windows (NETBIOS)

As portas de serviço do sistema também podem ser configuradas para permitir que um computador compartilhe sua conexão com a Internet com outros computadores conectados a ele pela mesma rede. Essa conexão, conhecida como ICS (Internet Connection Sharing), permite que o computador que está compartilhando a conexão atue como um gateway da Internet para os demais computadores em rede.

Observação: Se o computador tiver um aplicativo que aceite conexões de servidor FTP ou Web, o computador que compartilha a conexão poderá precisar abrir a porta de serviço do sistema associado e permitir o encaminhamento de conexões de entrada para essas portas.

Permitir acesso a uma porta de serviço do sistema existente

Você pode abrir uma porta existente para permitir acesso remoto ao serviço de rede no computador.

Observação: Uma porta de serviços do sistema aberta pode deixar seu computador vulnerável a ameaças à segurança vindas da Internet. Portanto, abra uma porta somente se necessário.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **Serviços do sistema**.
4. Em **Abrir porta de serviço do sistema**, selecione um serviço do sistema para abrir a porta.
5. Clique em **OK**.

Bloquear acesso a uma porta de serviço do sistema existente

Você pode fechar uma porta existente para bloquear acesso de rede remoto a um serviço no computador.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **Serviços do sistema**.
4. Em **Abrir porta de serviço do sistema**, desmarque um serviço do sistema para fechar sua respectiva porta.
5. Clique em **OK**.

Configurar uma nova porta de serviço do sistema

Você pode configurar uma nova porta de serviço de rede no computador que possa ser aberta ou fechada para permitir ou bloquear acesso remoto no computador.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **Serviços do sistema**.
4. Clique em **Adicionar**.
5. No painel Serviços do sistema, em **Portas e serviços do sistema**, digite o seguinte:
   - Nome do programa
   - Portas TCP/IP de entrada

- Portas TCP/IP de saída
- Portas UDP de entrada
- Portas UDP de saída

6 Se você desejar enviar informações de atividades dessa porta para outro computador com Windows da rede que compartilhe sua conexão com a Internet, selecione **Encaminhar a atividade de rede desta porta a usuários de rede que utilizem Internet Connection Sharing**.

7 Como opção, descreva a nova configuração.

8 Clique em **OK**.

Observação: Se o computador tiver um aplicativo que aceite conexões de servidor FTP ou Web, o computador que compartilha a conexão poderá precisar abrir a porta de serviço do sistema associado e permitir o encaminhamento de conexões de entrada para essas portas. Se estiver utilizando o Internet Connection Sharing (ICS), você também precisará adicionar uma conexão de computador confiável à lista Endereços IP confiáveis. Para obter mais informações, consulte Adicionar uma conexão de computador confiável.

Modificar uma porta de serviço do sistema

É possível modificar informações de acesso à rede de entrada e de saída sobre uma porta de serviço existente no sistema.

Observação: Se as informações da porta forem digitadas incorretamente, haverá falha no serviço do sistema.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.

2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.

3 No painel Firewall, clique em **Serviços do sistema**.

4 Selecione um serviço do sistema e clique em **Editar**.

5 No painel Serviços do sistema, em **Portas e serviços do sistema**, digite o seguinte:

- Nome do programa
- Portas TCP/IP de entrada
- Portas TCP/IP de saída
- Portas UDP de entrada
- Portas UDP de saída

6 Se você desejar enviar informações de atividades dessa porta para outro computador com Windows da rede que compartilhe sua conexão com a Internet, selecione **Encaminhar a atividade de rede desta porta a usuários de rede que utilizem Internet Connection Sharing**.
7 Como opção, descreva a configuração modificada.
8 Clique em **OK**.

Remover uma porta de serviço do sistema

Você pode remover do computador uma porta de serviço existente no sistema. Após a remoção, os computadores remotos não poderão mais acessar o serviço de rede em seu computador.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **Serviços do sistema**.
4 Selecione um serviço do sistema e clique em **Remover**.
5 Ao ser solicitado, clique em **Sim** para confirmar.

CAPÍTULO 20

Gerenciando conexões do computador

Você pode configurar o Firewall para gerenciar conexões remotas específicas com o seu computador criando regras baseadas em endereços IP, que são associados a computadores remotos. Computadores associados a endereços IP confiáveis podem se conectar ao seu computador, e endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de se conectarem ao seu computador.

O Ao permitir uma conexão, verifique se o computador em que está confiando é seguro. Se um computador no qual você confia for infectado por um worm ou outro mecanismo, você estará vulnerável à infecção. Além disso, a McAfee recomenda que os computadores confiáveis também sejam protegidos por um firewall e um programa antivírus atualizado. Firewall não registra tráfego nem gera alertas de eventos de endereços IP contidos na lista Endereços IP confiáveis.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Neste capítulo

Confiando em conexões de computador

Você pode adicionar, editar e remover endereços IP confiáveis no painel IPs confiáveis e proibidos, em **Endereços IP confiáveis**.

A lista **Endereços IP confiáveis** no painel IPs confiáveis e proibidos, permite que todo o tráfego de um computador específico chegue ao seu computador. O Firewall não registra tráfego nem gera alertas de eventos de endereços IP contidos na lista **Endereços IP confiáveis**.

O Firewall confia em todos os endereços IP selecionados da lista e sempre permite o tráfego de um IP confiável através do firewall em qualquer porta. Atividades entre um computador associado a um endereço IP confiável e o seu próprio computador não são filtradas nem analisadas pelo Firewall. Por padrão, os Endereços IP confiáveis listam a primeira rede privada encontrada pelo Firewall.

Ao permitir uma conexão, verifique se o computador em que está confiando é seguro. Se um computador no qual você confia for infectado por um worm ou outro mecanismo, você estará vulnerável à infecção. Além disso, a McAfee recomenda que os computadores confiáveis também sejam protegidos por um firewall e um programa antivírus atualizado.

Adicionar uma conexão de computador confiável

Você pode adicionar uma conexão de computador confiável e o endereço IP associado.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **IPs confiáveis e proibidos**.
4. No painel IPs confiáveis e proibidos, selecione **Endereços IP confiáveis** e clique em **Adicionar**.
5. Em **Adicionar regra de endereço IP confiável**, execute um dos procedimentos a seguir:
   - Selecione **Endereço IP único** e, em seguida, digite o endereço IP.
   - Selecione **Intervalo de endereços IP** e, em seguida, digite os endereços IP inicial e final nas caixas **Do endereço IP** e **Ao endereço IP**.

6 Se um serviço do sistema usar o ICS (Internet Connection Sharing), você poderá adicionar este intervalo de endereços IP: 192.168.0.1 a 192.168.0.255.
7 Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.
8 Como opção, digite uma descrição para a regra.
9 Clique em **OK**.
10 Na caixa de diálogo **IPs confiáveis e proibidos**, clique em **Sim** para confirmar.

Observação: Para obter mais informações sobre ICS (Internet Connection Sharing), consulte Configurar um novo serviço do sistema.

Adicionar um computador confiável a partir do registro de Eventos de entrada

Você pode adicionar uma conexão de computador confiável e seu endereço IP correspondente, a partir do registro de Eventos de entrada.

1 No painel do McAfee SecurityCenter, em Tarefas comuns, clique no **menu Avançado**.
2 Clique em **Relatórios e registros**.
3 Em **Eventos recentes**, clique em **Exibir registro**.
4 Clique em **Rede e Internet** e em **Eventos de entrada**.
5 Selecione um endereço IP de origem e, em **Desejo**, clique em **Confiar neste endereço**.
6 Clique em **Sim** para confirmar.

Editar uma conexão de computador confiável

Você pode editar uma conexão de computador confiável e o endereço IP associado.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **IPs confiáveis e proibidos**.
4 No painel IPs confiáveis e proibidos, selecione **Endereços IP confiáveis**.
5 Selecione um endereço IP e clique em **Editar**.
6 Em **Editar endereço IP confiável**, execute um dos procedimentos a seguir:
   - Selecione **Endereço IP único** e, em seguida, digite o endereço IP.

- Selecione **Intervalo de endereços IP** e, em seguida, digite os endereços IP inicial e final nas caixas **Do endereço IP** e **Ao endereço IP**.

7 Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.

8 Como opção, digite uma descrição para a regra.

9 Clique em **OK**.

Observação: Você não pode editar as conexões de computador padrão que o Firewall adicionou automaticamente, a partir de uma rede privada confiável.

Remover uma conexão de computador confiável

Você pode remover uma conexão de computador confiável e o endereço IP associado.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.

2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.

3 No painel Firewall, clique em **IPs confiáveis e proibidos**.

4 No painel IPs confiáveis e proibidos, selecione **Endereços IP confiáveis**.

5 Selecione um endereço IP e clique em **Remover**.

6 Na caixa de diálogo **IPs confiáveis e proibidos**, clique em **Sim** para confirmar.

Proibindo conexões de computador

Você pode adicionar, editar e remover endereços IP proibidos no painel IPs confiáveis e proibidos, em **Endereços IP proibidos**.

Computadores associados a endereços IP desconhecidos, suspeitos ou não confiáveis podem ser impedidos de conectar-se ao seu computador.

Como o Firewall bloqueia o tráfego indesejado, normalmente não é necessário proibir um endereço IP. Você deve proibir um endereço IP apenas quando está certo de que a conexão com a Internet representa uma ameaça específica. Tome o cuidado de não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP. Dependendo das configurações de segurança, o Firewall pode alertá-lo quando detectar um evento de um computador proibido.

Adicionar uma conexão de computador proibida

Você pode adicionar uma conexão de computador proibida e o endereço IP associado.

Observação: Tome cuidado para não bloquear endereços IP importantes, como os seus servidores DNS ou DHCP e outros servidores relacionados ao ISP.

1. No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3. No painel Firewall, clique em **IPs confiáveis e proibidos**.
4. No painel IPs confiáveis e proibidos, selecione **Endereços IP proibidos** e clique em **Adicionar**.
5. Em **Adicionar regra de endereço IP proibido**, execute um dos procedimentos a seguir:
   - Selecione **Endereço IP único** e, em seguida, digite o endereço IP.
   - Selecione **Intervalo de endereços IP** e, em seguida, digite os endereços IP inicial e final nas caixas **Do endereço IP** e **Ao endereço IP**.

6 Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.
7 Como opção, digite uma descrição para a regra.
8 Clique em **OK**.
9 Na caixa de diálogo **IPs confiáveis e proibidos**, clique em **Sim** para confirmar.

Editar uma conexão de computador proibida

Você pode editar uma conexão de computador proibida e o endereço IP associado.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **IPs confiáveis e proibidos**.
4 No painel IPs confiáveis e proibidos, selecione **Endereços IP proibidos** e clique em **Editar**.
5 Em **Editar endereço IP proibido**, execute um dos procedimentos a seguir:
   - Selecione **Endereço IP único** e, em seguida, digite o endereço IP.
   - Selecione **Intervalo de endereços IP** e, em seguida, digite os endereços IP inicial e final nas caixas **Do endereço IP** e **Ao endereço IP**.
6 Como opção, selecione **Regra expira em** e digite o número de dias durante os quais a regra deve ser aplicada.
7 Como opção, digite uma descrição para a regra.
8 Clique em **OK**.

Remover uma conexão de computador proibida

Você pode remover uma conexão de computador proibida e o endereço IP associado.

1 No painel do McAfee SecurityCenter, clique em **Rede e Internet** e clique em **Configurar**.
2 No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
3 No painel Firewall, clique em **IPs confiáveis e proibidos**.
4 No painel IPs confiáveis e proibidos, selecione **Endereços IP proibidos**.
5 Selecione um endereço IP e clique em **Remover**.
6 Na caixa de diálogo **IPs confiáveis e proibidos**, clique em **Sim** para confirmar.

Proibir um computador a partir do registro de Eventos de entrada

Você pode proibir uma conexão de computador confiável e seu endereço IP correspondente, a partir do registro de Eventos de entrada.

Endereços IP que aparecem no registro de Eventos de entrada são bloqueados. Portanto, a proibição de um endereço não acrescenta nenhuma proteção adicional, a não ser que o computador utilize portas que são deliberadamente abertas ou inclua um programa ao qual o acesso à Internet tenha sido permitido.

Adicione um endereço IP à lista **Endereços IP proibidos** somente se houver uma ou mais portas deliberadamente abertas e se houver necessidade de bloquear o acesso desse endereço às portas abertas.

É possível usar a página Eventos de entrada, que lista os endereços IP de todo o tráfego da Internet, para proibir um endereço IP suspeito de ser a origem de atividade suspeita ou não desejada na Internet.

1. No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique no **menu Avançado**.
2. Clique em **Relatórios e registros**.
3. Em **Eventos recentes**, clique em **Exibir registro**.
4. Clique em **Rede e Internet** e em **Eventos de entrada**.
5. Selecione um endereço IP de origem e, em **Desejo**, clique em **Proibir este endereço**.
6. Na caixa de diálogo **Adicionar regra de endereço IP proibido**, clique em **Sim** para confirmar.

Proibir um computador a partir do registro de Eventos de detecção de invasão

Você pode proibir uma conexão de computador confiável e seu endereço IP correspondente, a partir do registro de Eventos detecção de invasão.

1. No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique no **menu Avançado**.
2. Clique em **Relatórios e registros**.
3. Em **Eventos recentes**, clique em **Exibir registro**.
4. Clique em **Rede e Internet** e, em seguida, clique em **Eventos de detecção de invasão**.
5. Selecione um endereço IP de origem e, em **Desejo**, clique em **Proibir este endereço**.
6. Na caixa de diálogo **Adicionar regra de endereço IP proibido**, clique em **Sim** para confirmar.

CAPÍTULO 21

Registro, monitoramento e análise

O Firewall fornece análise, registros e monitoramento amplos e de fácil leitura para eventos e tráfego da Internet. Noções básicas sobre tráfego e eventos da Internet ajudam você a gerenciar suas conexões com a Internet.

Neste capítulo

Registro de eventos

O Firewall permite que você ative ou desative o registro de eventos e, se ativado, decida os tipos de evento que serão registrados. O registro de eventos permite que você verifique eventos recentes de entrada e de saída, bem como eventos de invasão.

Configurar registro de eventos

Você pode especificar e configurar os tipos de eventos de Firewall que serão registrados. Por padrão, o registro de eventos está ativado para todos os eventos e atividades.

1. No painel Configuração de Rede e Internet, em **Proteção de firewall ativada**, clique em **Avançado**.
2. No painel Firewall, clique em **Configurações do registro de eventos**.
3. Selecione a opção **Ativar o registro de eventos**, se ainda não estiver selecionada.
4. Em **Ativar o registro de eventos**, selecione ou remova os tipos de evento que deseja registrar. Os tipos de eventos incluem o seguinte:
   - Programas bloqueados
   - Pings ICMP
   - Tráfego de endereços IP proibidos
   - Eventos nas portas de serviço do sistema
   - Eventos em portas desconhecidas
   - Eventos da detecção de invasão (IDS)
5. Para impedir o registro em portas específicas, selecione **Não registrar eventos nas seguintes portas**, e digite números de porta únicos separados por vírgulas ou intervalos de portas separados por traços. Por exemplo, `137-139, 445, 400-5000`.
6. Clique em **OK**.

Exibir eventos recentes

Se o registro estiver ativado, você poderá exibir os eventos recentes. O painel Eventos recentes exibe a data e a descrição do evento. Ele exibe a atividade de programas que tiveram o acesso à Internet explicitamente bloqueado.

- No **menu Avançado**, no painel Tarefas comuns, clique em **Registros e relatórios** ou em **Exibir eventos recentes**. Uma alternativa é clicar em **Exibir eventos recentes** no painel Tarefas comuns do Menu básico.

Exibir eventos de entrada

Se o registro estiver ativado, é possível exibir os eventos de entrada. Os Eventos de entrada incluem data e a hora, endereços IP de origem, nome do host, tipo de evento e informações.

1 Assegure-se de que o menu Avançado esteja ativado. No painel Tarefas comuns, clique em **Relatórios e registros**.
2 Em **Eventos recentes**, clique em **Exibir registro**.
3 Clique em **Rede e Internet** e em **Eventos de entrada**.

Observação: Você pode confiar, proibir e rastrear um endereço IP a partir do registro de Eventos de entrada.

Exibir eventos de saída

Se o registro estiver ativado, é possível exibir os eventos de saída. Eventos de saída incluem o nome do programa que tenta acesso de saída, data e hora do evento e local do programa em seu computador.

1 No painel Tarefas comuns, clique em **Relatórios e registros**.
2 Em **Eventos recentes**, clique em **Exibir registro**.
3 Clique em **Rede e Internet** e em **Eventos de saída**.

Observação: Você pode permitir a um programa acesso total e somente de saída a partir do registro de Eventos de saída. Também é possível localizar informações adicionais sobre o programa.

Exibir eventos de detecção de invasão

Se o registro estiver ativado, será possível exibir os eventos de invasão de entrada. Os eventos de Detecção de invasão exibem a data e hora, o IP de origem, o nome do host do evento e o tipo de evento.

1 No painel Tarefas comuns, clique em **Relatórios e registros**.
2 Em **Eventos recentes**, clique em **Exibir registro**.
3 Clique em **Rede e Internet** e, em seguida, clique em **Eventos de detecção de invasão**.

Observação: Você pode proibir e rastrear um endereço IP a partir do registro de Eventos de detecção de invasão.

Trabalhando com estatísticas

O Firewall aproveita o site de segurança Hackerwatch da McAfee para fornecer estatísticas sobre eventos de segurança e atividades de porta globais da Internet.

Exibir estatística global dos eventos de segurança

O HackerWatch rastreia mundialmente eventos de segurança na Internet, e você pode exibi-los no SecurityCenter. As informações rastreadas listam os incidentes relatados ao HackerWatch nas últimas 24 horas, 7 dias, e 30 dias.

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Hackerwatch**.
3. Em Rastreamento de eventos, exiba estatísticas de eventos de segurança.

Exibir a atividade global de portas da Internet

O HackerWatch rastreia mundialmente eventos de segurança na Internet, e você pode exibi-los no SecurityCenter. As informações exibidas incluem os principais eventos de portas relatados ao HackerWatch durante os últimos sete dias. Normalmente, são exibidas informações de portas HTTP, TCP e UDP.

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Hackerwatch**.
3. Exiba os principais eventos de portas em **Atividade recente de porta**.

Rastreando tráfego da Internet

O Firewall oferece várias opções para rastrear o tráfego da Internet. Essas opções permitem que você rastreie geograficamente um computador da rede, obtenha informações de domínio e rede e rastreie computadores dos registros de Eventos de entrada e Eventos de detecção de invasão.

Rastrear geograficamente um computador da rede

Você pode usar o Rastreador visual para localizar geograficamente um computador que esteja se conectando ou tentando se conectar ao seu computador, usando o nome ou endereço IP dele. Também é possível acessar informações de rede e de inscrição com o Rastreador visual. O Rastreador visual exibe um mapa-múndi com a rota mais provável pela qual os dados estão trafegando entre o computador de origem e o seu computador.

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Rastreador visual**.
3. Digite o endereço IP do computador e clique em **Rastrear**.
4. Em **Rastreador visual**, selecione **Exibir mapa**.

Observação: Não é possível rastrear eventos de endereços IP em looping, privados ou inválidos.

Obter informações sobre a inscrição de um computador

Você pode obter as informações de inscrição de um computador no SecurityCenter, usando o Rastreador Visual. As informações incluem o nome de domínio, o nome e endereço do inscrito e o contato administrativo.

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Rastreador visual**.
3. Digite o endereço IP do computador e clique em **Rastrear**.
4. Em **Rastreador visual**, selecione **Exibir inscrito**.

Obter informações de rede de um computador

Você pode obter as informações de rede de um computador no SecurityCenter, usando o Rastreador Visual. As informações de rede incluem detalhes sobre a rede em que o domínio reside.

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Rastreador visual**.
3. Digite o endereço IP do computador e clique em **Rastrear**.
4. Em **Rastreador visual**, selecione **Exibir rede**.

Rastrear um computador a partir do registro de Eventos de entrada

No painel Eventos de entrada, você pode rastrear um endereço IP que aparece no registro de Eventos de entrada.

1. Assegure-se de que o menu Avançado esteja ativado. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Clique em **Rede e Internet** e em **Eventos de entrada**.
4. No painel Eventos de entrada, selecione um endereço IP de origem e clique em **Rastrear este endereço**.
5. No painel do Rastreador visual, clique em umas destas opções:
   - **Exibir mapa**: Localizar geograficamente um computador, usando o endereço IP selecionado.
   - **Exibição do inscrito**: Localizar informações de domínio, usando o endereço IP selecionado.
   - **Exibição da rede**: Localizar informações de rede, usando o endereço IP selecionado.
6. Clique em **Concluído**.

Rastrear um computador a partir do registro de Eventos de detecção de invasão

No painel Eventos de detecção de invasão, você pode rastrear um endereço IP que aparece no registro de Eventos de detecção de invasão.

1. No painel Tarefas comuns, clique em **Relatórios e registros**.
2. Em **Eventos recentes**, clique em **Exibir registro**.
3. Clique em **Rede e Internet** e, em seguida, clique em **Eventos de detecção de invasão**. No painel Eventos de detecção de invasão, selecione um endereço IP de origem e clique em **Rastrear este endereço**.
4. No painel do Rastreador visual, clique em umas destas opções:
   - **Exibir mapa**: Localizar geograficamente um computador, usando o endereço IP selecionado.
   - **Exibição do inscrito**: Localizar informações de domínio, usando o endereço IP selecionado.
   - **Exibição da rede**: Localizar informações de rede, usando o endereço IP selecionado.
5. Clique em **Concluído**.

Rastrear um endereço IP monitorado

É possível rastrear um endereço IP monitorado, para obter uma exibição geográfica que mostre a rota mais provável dos dados, do computador de origem até o seu. Além disso, você pode obter informações de inscrição e de rede sobre o endereço IP.

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Monitor de tráfego**.
3. Em **Monitor de tráfego**, clique em **Programas ativos**.
4. Selecione um programa e o endereço IP que aparece abaixo do nome do programa.
5. Em **Atividade do programa**, clique em **Rastrear este IP**.
6. Em **Rastreador visual**, você pode ver um mapa que exibe a rota mais provável pela qual os dados estão trafegando entre o computador de origem e o seu computador. Além disso, você pode obter informações de inscrição e de rede sobre o endereço IP.

Observação: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Rastreador visual**.

Monitorando tráfego da Internet

O Firewall fornece vários métodos para monitorar seu tráfego da Internet, inclusive os seguintes:

- **Gráfico de análise do tráfego**: Exibe tráfego recente de entrada e saída da Internet.
- **Gráfico de utilização do tráfego**: Exibe a porcentagem da largura de banda usada pelos programas mais ativos nas últimas 24 horas.
- **Programas ativos**: Exibe os programas que atualmente usam o maior número de conexões de rede em seu computador e quais endereços IP são acessados pelos programas.

Sobre o Gráfico de análise de tráfego

O gráfico de Análise de tráfego é uma representação numérica e gráfica do tráfego de entrada e saída da Internet. Ele também mostra quais programas estão usando o maior número de conexões de rede em seu computador e os endereços IP que o programa acessa.

No painel Análise de tráfego, é possível exibir tráfego recente de entrada e saída na Internet e taxas de transferência atuais, médias e máximas. Você também pode exibir o volume de tráfego, inclusive a quantidade de tráfego desde que o firewall foi iniciado, além do tráfego total do mês corrente e dos meses anteriores.

O painel Análise de tráfego exibe a atividade de Internet do computador em tempo real, incluindo o volume e taxa de tráfego recente de entrada e saída de Internet, velocidade da conexão e total de bytes transferidos pela Internet.

A linha verde sólida representa a taxa atual de transferência do tráfego de entrada. A linha verde pontilhada representa a taxa média de transferência do tráfego de entrada. Se a taxa atual de transferência e a taxa média de transferência forem iguais, a linha pontilhada não será exibida no gráfico. A linha sólida representará duas taxas de transferência: a média e a atual.

A linha vermelha sólida representa a taxa atual de transferência do tráfego de saída. A linha vermelha pontilhada representa a taxa média de transferência do tráfego de saída. Se a taxa atual de transferência e a taxa média de transferência forem iguais, a linha pontilhada não será exibida no gráfico. A linha sólida representará duas taxas de transferência: a média e a atual.

Analisar tráfego de entrada e de saída

O gráfico de Análise de tráfego é uma representação numérica e gráfica do tráfego de entrada e saída da Internet. Ele também mostra quais programas estão usando o maior número de conexões de rede em seu computador e os endereços IP que o programa acessa.

1 Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2 No painel Ferramentas, clique em **Monitor de tráfego**.
3 Em **Monitor de tráfego**, clique em **Análise de tráfego**.

Dica: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Análise de tráfego**.

Monitorar largura de banda de um programa

Você pode visualizar um gráfico de torta, que exibe a porcentagem aproximada de largura de banda usada pelos programas mais ativos em seu computador durante as últimas vinte e quatro horas. O gráfico oferece uma representação visual das quantidades relativas de largura de banda usada pelos programas.

1 Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2 No painel Ferramentas, clique em **Monitor de tráfego**.
3 Em **Monitor de tráfego**, clique em **Utilização de tráfego**.

Dica: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Utilização de tráfego**.

Monitorar a atividade de um programa

Você pode exibir a atividade de entrada e saída dos programas, que exibe conexões e portas de computadores remotos.

1 Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2 No painel Ferramentas, clique em **Monitor de tráfego**.
3 Em **Monitor de tráfego**, clique em **Programas ativos**.
4 Você pode exibir as seguintes informações:
   - Gráfico de atividades do programa: Selecione um programa para exibir um gráfico de suas atividades.
   - Conexão de escuta: Selecione um item de Escuta sob o nome do programa.
   - Conexão do computador: Selecione um endereço IP sob o nome do programa, serviço ou processo do sistema.

Observação: Para exibir as estatísticas mais atualizadas, clique em **Atualizar**, em **Programas ativos**.

CAPÍTULO 22

Saiba mais sobre segurança da Internet

O Firewall utiliza o site de segurança da McAfee, Hackerwatch, para fornecer informações atualizadas sobre programas e atividade global da Internet. O Hackerwatch também fornece um tutorial em HTML sobre o Firewall.

Neste capítulo

Iniciar o tutorial do Hackerwatch

Para aprender sobre o Firewall, você pode acessar o tutorial do Hackerwatch a partir do SecurityCenter.

1. Verifique se o Menu avançado está ativado e clique em **Ferramentas**.
2. No painel Ferramentas, clique em **Hackerwatch**.
3. Em **Recursos do Hackerwatch**, clique em **Exibir tutorial**.

C A P Í T U L O 2 3

McAfee QuickClean

O QuickClean melhora o desempenho do computador excluindo arquivos que possam criar resíduos. Ele esvazia a Lixeira e exclui arquivos temporários, atalhos, fragmentos de arquivos perdidos, arquivos de registro, arquivos em cache, cookies, arquivos do histórico do navegador, emails excluídos e enviados, arquivos usados recentemente, arquivos do Active-X e arquivos de ponto de restauração do sistema. O QuickClean também protege a sua privacidade usando o componente McAfee Shredder para excluir de forma segura e permanente itens que possam conter informações pessoais sigilosas, como seu nome e seu endereço. Para obter informações sobre como destruir arquivos, consulte o McAfee Shredder.

O Desfragmentador de disco organiza os arquivos e as pastas no computador para garantir que eles não se espalhem (ou seja, que fiquem fragmentados) quando forem salvos na unidade de disco rígido. Ao desfragmentar a unidade de disco rígido periodicamente, você garante que arquivos e pastas fragmentados sejam consolidados para uma recuperação rápida no futuro.

Se não quiser fazer a manutenção manual do computador, você poderá programar o QuickClean e o Desfragmentador de disco para serem executados automaticamente, como tarefas independentes, com a freqüência desejada.

Observação: O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician.

Neste capítulo

Recursos do QuickClean

O QuickClean fornece vários limpadores que excluem arquivos desnecessários com segurança e eficiência. Ao excluir esses arquivos, você aumenta o espaço na unidade de disco rígido e melhora o desempenho do computador.

Limpando o computador

O QuickClean exclui arquivos que possam criar resíduos no computador. Ele esvazia a Lixeira e exclui arquivos temporários, atalhos, fragmentos de arquivos perdidos, arquivos de registro, arquivos em cache, cookies, arquivos do histórico do navegador, emails excluídos e enviados, arquivos usados recentemente, arquivos do Active-X e arquivos de ponto de restauração do sistema. O QuickClean exclui esses itens sem afetar outras informações essenciais.

Você pode usar qualquer um dos limpadores do QuickClean para excluir arquivos desnecessários do computador. A tabela a seguir descreve os limpadores do QuickClean:

Nome	Função
Limpador da Lixeira	Exclui os arquivos da Lixeira.
Limpador de arquivos temporários	Exclui os arquivos armazenados nas pastas temporárias.
Limpador de atalhos	Exclui atalhos que não funcionam e atalhos que não estão associados a um programa.
Limpador de fragmentos de arquivos perdidos	Exclui os fragmentos de arquivos perdidos do computador.
Limpador de registro	Exclui informações do Registro do Windows® de programas que não existem mais no computador. O Registro é um banco de dados no qual o Windows armazena suas informações de configuração. O Registro contém perfis para cada usuário do computador e informações sobre as configurações de propriedade, os programas instalados e o hardware do sistema. O Windows sempre consulta essas informações durante seu funcionamento.
Limpador de cache	Exclui os arquivos em cache que se acumulam quando você navega na Internet. Geralmente, esses arquivos são armazenados como arquivos temporários em uma pasta de cache. A pasta de cache é uma área de armazenamento temporário no computador. Para aumentar a velocidade e a eficiência da navegação na Internet, seu navegador poderá recuperar uma página da Web do respectivo cache (em vez de recuperá-la de um servidor remoto) na próxima vez que você quiser visualizá-la.

Nome	Função
Limpador de cookies	Exclui cookies. Geralmente, esses arquivos são armazenados como arquivos temporários. Um cookie é um pequeno arquivo que contém informações, que geralmente incluem um nome de usuário e a data e a hora atuais, e é armazenado no computador de uma pessoa que está navegando na Internet. Os cookies são usados principalmente por sites para identificar os usuários que se registraram no site ou que o visitaram anteriormente. Contudo, eles também podem ser uma fonte de informação para hackers.
Limpador de histórico do navegador	Exclui o histórico do navegador da Web.
Limpador de emails do Outlook Express e do Outlook (itens excluídos e enviados)	Apaga emails excluídos e enviados do Outlook® e do Outlook Express.
Limpador usado recentemente	Exclui arquivos usados recentemente que tenham sido criados com um destes programas: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
Limpador do ActiveX	Exclui controles ActiveX. O ActiveX é um componente de software usado por programas ou páginas da Web para adicionar funcionalidades que se misturam e são exibidas como uma parte normal do programa ou da página da Web. A maioria dos controles ActiveX é inofensiva, porém, alguns deles podem capturar informações do seu computador.

Nome	Função
Limpador do ponto de restauração do sistema	Exclui do computador pontos de restauração do sistema antigos (exceto o mais recente). Os pontos de restauração do sistema são criados pelo Windows para marcar quaisquer alterações feitas no computador. Desse modo, você poderá voltar ao estado anterior caso ocorra algum problema.

Limpar o computador

Você pode usar qualquer um dos limpadores do QuickClean para excluir arquivos desnecessários do computador. Quando terminar, em **Resumo do QuickClean**, você poderá visualizar a quantidade de espaço em disco recuperado depois da limpeza, o número de arquivos excluídos, bem como a data e a hora de execução da última operação do QuickClean.

1 No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
2 Em **McAfee QuickClean**, clique em **Iniciar**.
3 Siga um destes procedimentos:
   - Clique em **Avançar** para aceitar os limpadores padrão da lista.
   - Marque ou desmarque os limpadores apropriados e, em seguida, clique em **Avançar.** Se selecionar a opção Limpador usado recentemente, clique em **Propriedades** para marcar ou desmarcar os arquivos criados recentemente com os programas da lista. Em seguida, clique em **OK**.
   - Clique em **Restaurar padrões** para restaurar os limpadores padrão e, em seguida, clique em **Avançar**.
4 Depois que a análise for realizada, clique em **Avançar**.
5 Clique em **Avançar** para confirmar a exclusão do arquivo.
6 Siga um destes procedimentos:
   - Clique em **Avançar** para aceitar o padrão **Não, desejo excluir os arquivos usando a exclusão padrão do Windows**.
   - Clique em **Sim, desejo apagar com segurança os meus arquivos usando o Shredder**, especifique o número de etapas, até 10, e clique em **Avançar**. Se o volume de informações a ser apagado for muito grande, a destruição dos arquivos poderá ser um processo longo.

7. Se algum arquivo ou item for bloqueado durante a limpeza, talvez você seja solicitado a reiniciar o computador. Clique em **OK** para fechar o prompt.
8. Clique em **Concluir**.

Observação: Os arquivos excluídos com o Shredder não podem ser recuperados. Para obter informações sobre como destruir arquivos, consulte o McAfee Shredder.

Desfragmentando o computador

O Desfragmentador de disco organiza os arquivos e as pastas no computador para garantir que eles não se espalhem (ou seja, que fiquem fragmentados) quando forem salvos na unidade de disco rígido. Ao desfragmentar a unidade de disco rígido periodicamente, você garante que arquivos e pastas fragmentados sejam consolidados para uma recuperação rápida no futuro.

Desfragmentar o computador

Você pode desfragmentar o computador para melhorar a recuperação de pastas e arquivos e o acesso a eles.

1. No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
2. Em **Desfragmentador de disco**, clique em **Analisar**.
3. Siga as instruções na tela.

Observação: Para obter mais informações sobre o Desfragmentador de disco, consulte a Ajuda do Windows.

Programando uma tarefa

O Programador de tarefas automatiza a freqüência com que o QuickClean ou o Desfragmentador de disco é executado no computador. Por exemplo, você pode programar uma tarefa do QuickClean para esvaziar a Lixeira todos os domingos às 21:00 ou pode programar uma tarefa do Desfragmentador de disco para desfragmentar a unidade de disco rígido do computador no último dia de cada mês. É possível criar, modificar ou excluir uma tarefa a qualquer momento. Para que a tarefa programada seja executada, é preciso que você esteja conectado ao computador. Se por algum motivo uma tarefa não for executada, ela será reprogramada para cinco minutos depois que você fizer logon novamente.

Programar uma tarefa do QuickClean

Você pode programar uma tarefa do QuickClean para limpar automaticamente o computador usando um ou mais limpadores. Quando terminar, em **Resumo do QuickClean**, você poderá visualizar a data e a hora em que a tarefa está programada para ser executada novamente.

1 Abra o painel do Programador de tarefas.

   Como?

   1. No McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
   2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Selecionar operação a ser programada**, clique em **McAfee QuickClean**.

3 Digite um nome para a tarefa na caixa **Nome da tarefa** e clique em **Criar**.

4 Siga um destes procedimentos:

   - Clique em **Avançar** para aceitar os limpadores da lista.
   - Marque ou desmarque os limpadores apropriados e, em seguida, clique em **Avançar**. Se selecionar a opção Limpador usado recentemente, clique em **Propriedades** para marcar ou desmarcar os arquivos criados recentemente com os programas da lista. Em seguida, clique em **OK**.
   - Clique em **Restaurar padrões** para restaurar os limpadores padrão e, em seguida, clique em **Avançar**.

5 Siga um destes procedimentos:

   - Clique em **Programação** para aceitar o padrão **Não, desejo excluir os arquivos usando a exclusão padrão do Windows**.

- Clique em **Sim, desejo apagar com segurança os meus arquivos usando o Shredder**, especifique o número de etapas, até 10, e clique em **Programação**.

6 Na caixa de diálogo **Programação**, selecione a freqüência com que a tarefa deverá ser executada e, em seguida, clique em **OK**.

7 Se tiver feito alterações nas propriedades do Limpador usado recentemente, você poderá ser solicitado a reiniciar o computador. Clique em **OK** para fechar o prompt.

8 Clique em **Concluir**.

Observação: Os arquivos excluídos com o Shredder não podem ser recuperados. Para obter informações sobre como destruir arquivos, consulte o McAfee Shredder.

Modificar uma tarefa do QuickClean

Você pode modificar uma tarefa programada do QuickClean para mudar os limpadores utilizados ou a freqüência com que ela é executada automaticamente no computador. Quando terminar, em **Resumo do QuickClean**, você poderá visualizar a data e a hora em que a tarefa está programada para ser executada novamente.

1 Abra o painel do Programador de tarefas.

Como?

1. No McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Selecionar operação a ser programada**, clique em **McAfee QuickClean**.

3 Selecione a tarefa na lista **Selecionar uma tarefa existente** e clique em **Modificar**.

4 Siga um destes procedimentos:

- Clique em **Avançar** para aceitar os limpadores selecionados para a tarefa.
- Marque ou desmarque os limpadores apropriados e, em seguida, clique em **Avançar**. Se selecionar a opção Limpador usado recentemente, clique em **Propriedades** para marcar ou desmarcar os arquivos criados recentemente com os programas da lista. Em seguida, clique em **OK**.
- Clique em **Restaurar padrões** para restaurar os limpadores padrão e, em seguida, clique em **Avançar**.

5 Siga um destes procedimentos:

- Clique em **Programação** para aceitar o padrão **Não, desejo excluir os arquivos usando a exclusão padrão do Windows**.
- Clique em **Sim, desejo apagar com segurança os meus arquivos usando o Shredder**, especifique o número de etapas, até 10, e clique em **Programação**.

6 Na caixa de diálogo **Programação**, selecione a freqüência com que a tarefa deverá ser executada e, em seguida, clique em **OK**.

7 Se tiver feito alterações nas propriedades do Limpador usado recentemente, você poderá ser solicitado a reiniciar o computador. Clique em **OK** para fechar o prompt.

8 Clique em **Concluir**.

Observação: Os arquivos excluídos com o Shredder não podem ser recuperados. Para obter informações sobre como destruir arquivos, consulte o McAfee Shredder.

Excluir uma tarefa do QuickClean

Você poderá excluir uma tarefa programada do QuickClean se não quiser mais que ela seja executada automaticamente.

1 Abra o painel do Programador de tarefas.

Como?

1. No McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Selecionar operação a ser programada**, clique em **McAfee QuickClean**.

3 Selecione a tarefa na lista **Selecionar uma tarefa existente**.

4 Clique em **Excluir** e, em seguida, clique em **Sim** para confirmar a exclusão.

5 Clique em **Concluir**.

Programar uma tarefa do Desfragmentador de disco

Você pode programar uma tarefa do Desfragmentador de disco para definir a freqüência com que a unidade de disco rígido do computador será desfragmentada automaticamente. Quando terminar, em **Desfragmentador de disco**, você poderá visualizar a data e a hora em que a tarefa está programada para ser executada novamente.

1 Abra o painel do Programador de tarefas.

    Como?

    1. No McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
    2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Selecionar operação a ser programada**, clique em **Desfragmentador de disco**.

3 Digite um nome para a tarefa na caixa **Nome da tarefa** e clique em **Criar**.

4 Siga um destes procedimentos:

- Clique em **Programação** para aceitar a opção padrão **Realizar a desfragmentação mesmo se houver pouco espaço livre**.
- Desmarque a opção **Realizar a desfragmentação mesmo se houver pouco espaço livre** e clique em **Programação**.

5 Na caixa de diálogo **Programação**, selecione a freqüência com que a tarefa deverá ser executada e, em seguida, clique em **OK**.

6 Clique em **Concluir**.

Modificar uma tarefa do Desfragmentador de disco

Você pode modificar uma tarefa programada do Desfragmentador de disco para mudar a freqüência com que ela é executada automaticamente no computador. Quando terminar, em **Desfragmentador de disco**, você poderá visualizar a data e a hora em que a tarefa está programada para ser executada novamente.

1 Abra o painel do Programador de tarefas.

    Como?

1. No McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Selecionar operação a ser programada**, clique em **Desfragmentador de disco**.

3 Selecione a tarefa na lista **Selecionar uma tarefa existente** e clique em **Modificar**.

4 Siga um destes procedimentos:

- Clique em **Programação** para aceitar a opção padrão **Realizar a desfragmentação mesmo se houver pouco espaço livre**.
- Desmarque a opção **Realizar a desfragmentação mesmo se houver pouco espaço livre** e clique em **Programação**.

5 Na caixa de diálogo **Programação**, selecione a freqüência com que a tarefa deverá ser executada e, em seguida, clique em **OK**.

6 Clique em **Concluir**.

Excluir uma tarefa do Desfragmentador de disco

Você poderá excluir uma tarefa programada do Desfragmentador de disco se não quiser mais que ela seja executada automaticamente.

1 Abra o painel do Programador de tarefas.

Como?

1. No McAfee SecurityCenter, em **Tarefas comuns**, clique em **Manter o computador**.
2. Em **Programador de tarefas**, clique em **Iniciar**.

2 Na lista **Selecionar operação a ser programada**, clique em **Desfragmentador de disco**.

3 Selecione a tarefa na lista **Selecionar uma tarefa existente**.

4 Clique em **Excluir** e, em seguida, clique em **Sim** para confirmar a exclusão.

5 Clique em **Concluir**.

CAPÍTULO 24

McAfee Shredder

O McAfee Shredder exclui (ou destrói) itens definitivamente da unidade de disco rígido do computador. Mesmo se você excluir seus arquivos e pastas manualmente e esvaziar a Lixeira, ou excluir a pasta Arquivos temporários da Internet, ainda assim é possível recuperar essas informações, usando as ferramentas de análise forense do computador. Além disso, um arquivo excluído pode ser recuperado, porque alguns programas fazem cópias temporárias e ocultas de arquivos abertos. O Shredder protege a sua privacidade, excluindo esses arquivos indesejados de forma segura e permanente. É importante lembrar que arquivos destruídos não podem ser restaurados.

Observação: O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician.

Neste capítulo

Recursos do Shredder

O Shredder exclui itens da unidade de disco rígido do computador, por isso as informações associadas a eles não podem ser recuperadas. Ele protege a sua privacidade de forma segura e definitiva excluindo arquivos e pastas, itens da lixeira e da pasta Arquivos temporários da Internet, além de todo o conteúdo dos discos do computador, como CDs regraváveis, unidades de disco externas e disquetes.

Destruindo arquivos, pastas e discos

O Shredder garante que as informações contidas nos arquivos e pastas excluídos da Lixeira e da pasta Arquivos temporários da Internet não possa ser recuperado, mesmo com ferramentas especiais. Com o Shredder, você pode especificar em quantas etapas (até 10) deseja que um item seja destruído. Um número superior de etapas de destruição aumenta o nível de exclusão do arquivo de segurança.

Destruir arquivos e pastas

Você pode destruir arquivos e pastas da unidade de disco rígido do computador, incluindo os itens da Lixeira e da pasta Arquivos temporários da Internet.

1 Abrir o **Shredder**:

   Como?

   1. No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique no **menu Avançado**.
   2. No painel esquerdo, clique em **Ferramentas**.
   3. Clique em **Shredder**.

2 No painel Destruir arquivos e pastas, em **Desejo**, clique em **Apagar arquivos e pastas**.

3 Em **Nível de destruição**, escolha um dos seguintes níveis de destruição:

   - **Rápida**: Destrói os itens selecionados em apenas uma etapa.
   - **Abrangente**: Destrói os itens selecionados em sete etapas.
   - **Personalizada**: Destrói os itens selecionados em até dez etapas.

4 Clique em **Avançar**.

5 Escolha uma das seguintes opções:

   - Na lista **Selecione os arquivos a serem destruídos**, clique em **Conteúdo da Lixeira** ou em **Arquivos temporários da Internet**.
   - Clique em **Procurar**, navegue até o arquivo que deseja destruir, selecione-o e clique em **Abrir**.

6 Clique em **Avançar**.
7 Clique em **Iniciar**.
8 Quando o Shredder terminar, clique em **Concluído**.

Observação: Não trabalhe com nenhum arquivo até o Shredder concluir a tarefa.

Destruir um disco inteiro

Você pode destruir todo o conteúdo de um disco em apenas uma etapa. Somente unidades removíveis, como unidades de disco externas, CDs graváveis e disquetes podem ser destruídas.

1 Abrir o **Shredder**:

   Como?

   1. No painel do McAfee SecurityCenter, em **Tarefas comuns**, clique no **menu Avançado**.
   2. No painel esquerdo, clique em **Ferramentas**.
   3. Clique em **Shredder**.

2 No painel Destruir arquivos e pastas, em **Desejo**, clique em **Apagar um disco inteiro**.
3 Em **Nível de destruição**, escolha um dos seguintes níveis de destruição:
   - **Rápida**: Destrói a unidade selecionada em apenas uma etapa.
   - **Abrangente**: Destrói a unidade selecionada em sete etapas.
   - **Personalizada**: Destrói a unidade selecionada em até dez etapas.
4 Clique em **Avançar**.
5 Na lista **Selecione o disco**, clique na unidade que deseja destruir.
6 Clique em **Avançar** e em **Sim** para confirmar.
7 Clique em **Iniciar**.
8 Quando o Shredder terminar, clique em **Concluído**.

Observação: Não trabalhe com nenhum arquivo até o Shredder concluir a tarefa.

CAPÍTULO 25

McAfee Network Manager

O Network Manager apresenta uma exibição gráfica dos computadores e componentes que formam sua rede doméstica. Você pode usar o Network Manager para monitorar remotamente o status de proteção de cada computador gerenciado da sua rede e para corrigir remotamente as vulnerabilidades de segurança relatadas nesses computadores.

Antes de usar o Network Manager, você pode se familiarizar com alguns dos recursos. A Ajuda do Network Manager fornece detalhes sobre como configurar e usar esses recursos.

Observação: O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician.

Neste capítulo

Recursos do Network Manager

O Network Manager oferece os seguintes recursos.

Mapa gráfico da rede

O mapa de rede do Network Manager oferece uma representação gráfica do status de proteção dos computadores e componentes que formam sua rede doméstica. Quando você faz modificações na rede (adicionando um computador, por exemplo), o mapa de rede reconhece essas alterações. Você pode atualizar o mapa de rede, renomear a rede e mostrar ou ocultar componentes do mapa de rede, para personalizar sua exibição. Também é possível exibir os detalhes de qualquer um dos componentes no mapa de rede.

Gerenciamento remoto

Use o mapa de rede do Network Manager para gerenciar o status de proteção dos computadores que formam sua rede doméstica. Você pode convidar um computador a associar-se à rede gerenciada, monitorar o status de segurança dos computadores gerenciados e corrigir vulnerabilidades de segurança conhecidas a partir de um computador remoto da rede.

Noções básicas sobre os ícones do Network Manager

A tabela a seguir descreve os ícones geralmente usados no mapa de rede do Network Manager.

Ícone	Descrição
	Representa um computador gerenciado on-line
	Representa um computador gerenciado que está off-line
	Representa um computador não gerenciado com o SecurityCenter instalado
	Representa um computador não gerenciado que está off-line
	Representa um computador que está on-line e não tem o SecurityCenter instalado, ou um dispositivo de rede desconhecido
	Representa um computador que está off-line e não tem o SecurityCenter instalado, ou um dispositivo de rede desconhecido off-line
	Significa que o item correspondente está protegido e conectado
	Significa que o item correspondente pode exigir a sua atenção
	Significa que o item correspondente exige atenção imediata
	Representa um roteador doméstico sem fio
	Representa um roteador doméstico padrão
	Representa a Internet, quando conectada
	Representa a Internet, quando desconectada

CAPÍTULO 26

Configurando uma rede gerenciada

Para configurar uma rede gerenciada, trabalhe com os itens de seu mapa de rede e adicione membros (computadores) a ela. Para que um computador possa ser gerenciado à distância ou receba permissão para gerenciar outros computadores da rede, ele precisa se tornar um membro confiável da rede. A associação à rede é concedida a novos computadores por membros existentes (computadores) da rede com permissões administrativas.

Você pode exibir os detalhes associados a qualquer um dos componentes mostrados no mapa de rede, mesmo depois de fazer alterações na rede (adicionando um computador, por exemplo).

Neste capítulo

Trabalhando com o mapa de rede

Quando você conecta um computador à rede, o Network Manager analisa a rede para determinar se há algum membro gerenciado ou não, os atributos do roteador e o status da Internet. Se nenhum membro for encontrado, o Network Manager presume que o computador conectado no momento é o primeiro computador da rede e transforma esse computador em membro gerenciado com permissões administrativas. Por padrão, o nome da rede inclui o grupo de trabalho ou o domínio do primeiro computador conectado à rede, que tenha o SecurityCenter instalado. Contudo, você pode renomear a rede a qualquer momento.

Quando faz modificações na rede (adicionando um computador, por exemplo), você pode personalizar o mapa de rede. Por exemplo, você pode atualizar o mapa de rede, renomear a rede e mostrar ou ocultar componentes do mapa de rede a fim de personalizar sua exibição. Também é possível exibir os detalhes associados a qualquer dos componentes exibidos no mapa de rede.

Acessar o mapa de rede

O mapa de rede oferece uma representação gráfica dos computadores e componentes que fazem parte de sua rede doméstica.

- No menu Avançado ou Básico, clique em **Gerenciar rede**.

Observação: Quando acessar o mapa de rede pela primeira vez, você será solicitado a confiar nos outros computadores da rede.

Atualizar o mapa de rede

Você pode atualizar o mapa da rede a qualquer momento, por exemplo, depois que outro computador associa-se à rede gerenciada.

1. No menu Avançado ou Básico, clique em **Gerenciar rede**.
2. Clique em **Atualizar o mapa de rede** em **Desejo**.

Observação: O link **Atualizar o mapa de rede** só estará disponível se não houver itens selecionados no mapa de rede. Para limpar um item, clique no item selecionado ou clique em uma área em branco no mapa de rede.

Renomear a rede

Por padrão, o nome da rede inclui o grupo de trabalho ou nome de domínio do primeiro computador conectado à rede que tenha o SecurityCenter instalado. Se preferir usar outro nome, você pode alterá-lo.

1 No menu Avançado ou Básico, clique em **Gerenciar rede**.
2 Clique em **Renomear a rede** em **Desejo**.
3 Digite o nome da rede na caixa **Nome da rede**.
4 Clique em **OK**.

Observação: O link **Renomear a rede** só estará disponível se não houver itens selecionados no mapa de rede. Para limpar um item, clique no item selecionado ou clique em uma área em branco no mapa de rede.

Mostrar ou ocultar um item no mapa de rede

Por padrão, todos os computadores e componentes de sua rede doméstica são exibidos no mapa de rede. Porém, se algum item tiver sido ocultado, você poderá mostrá-lo novamente a qualquer momento. Somente os itens não gerenciados podem ser ocultados; não é possível ocultar os computadores gerenciados.

Para...	No menu Básico ou Avançado, clique em **Gerenciar Rede** e execute um dos procedimentos a seguir...
Ocultar um item do mapa de rede	Clique em um item do mapa de rede e clique em **Ocultar este item** em **Desejo**. Na caixa de diálogo de confirmação, clique em **Sim**.
Mostrar itens ocultos no mapa de rede	Em **Desejo**, clique em **Mostrar itens ocultos**.

Exibir detalhes de um item

Você poderá exibir informações detalhadas sobre qualquer componente em sua rede se selecioná-lo no mapa de rede. Essas informações incluem o nome do componente, seu status de proteção e outras informações necessárias para gerenciar o componente.

1 Clique no ícone do item no mapa de rede.
2 Em **Detalhes**, veja as informações sobre o item.

Associando à rede gerenciada

Para que um computador possa ser gerenciado à distância ou receba permissão para gerenciar outros computadores da rede, ele precisa se tornar um membro confiável da rede. A associação à rede é concedida a novos computadores por membros existentes (computadores) da rede com permissões administrativas. Para garantir que apenas computadores confiáveis se associem à rede, os usuários do computador concedente e do computador que está se associando precisam autenticar um ao outro.

Quando um computador se associa à rede, ele é solicitado a expor seu status de proteção McAfee aos outros computadores da rede. Se um computador aceita expor seu status de proteção, ele se torna um membro gerenciado da rede. Se um computador se recusa a expor seu status de proteção, ele se torna um membro não gerenciado da rede. Membros não gerenciados da rede normalmente são computadores convidados que desejam acessar outros recursos da rede (enviar arquivos ou compartilhar impressoras, por exemplo).

Observação: Depois que se associar, se você tiver outros programas de rede da McAfee instalados (o EasyNetwork, por exemplo), o computador também será reconhecido como membro gerenciado nesses programas. O nível de permissão atribuído a um computador no Network Manager se aplica a todos os programas de rede McAfee. Para obter mais informações sobre o que significam permissões de convidado, total ou administrativa em outros programas de rede da McAfee, consulte a documentação fornecida com o programa.

Associar-se a uma rede gerenciada

Quando recebe um convite para se associar a uma rede gerenciada, você pode aceitá-lo ou rejeitá-lo. Você também pode determinar se deseja que esse computador e outros computadores da rede monitorem as configurações de segurança uns dos outros (por exemplo, se os serviços de proteção contra vírus de um computador estão atualizados).

1. Na caixa de diálogo Rede gerenciada, verifique se a caixa de seleção **Permitir que todos os computadores desta rede monitorem configurações de segurança** está marcada.
2. Clique em **Associar**.
   Quando você aceita o convite, duas cartas de baralho são exibidas.
3. Confirme se as cartas são as mesmas que estão sendo exibidas no computador que enviou o convite para você se associar à rede gerenciada.
4. Clique em **OK**.

Observação: Se o computador que convidou você para associar-se à rede gerenciada não estiver exibindo as mesmas cartas de baralho exibidas na caixa de diálogo de confirmação de segurança, houve uma violação na segurança da rede gerenciada. Associar-se à rede pode colocar seu computador em risco; por isso, clique em **Cancelar** na caixa de diálogo Rede gerenciada.

Convidar um computador para associar-se à rede gerenciada

Se um computador for adicionado à rede gerenciada, ou se outro computador não gerenciado existir na rede, você poderá convidá-lo a associar-se à rede gerenciada. Apenas computadores com permissões administrativas na rede podem convidar outros computadores para se associar. Ao enviar o convite, você também deve especificar o nível de permissão que deseja atribuir ao novo computador.

1. Clique no ícone correspondente a um computador não gerenciado no mapa de rede.
2. Clique em **Monitorar este computador**, em **Desejo**.
3. Na caixa de diálogo Convidar um computador para associar-se à rede gerenciada, execute um dos seguintes procedimentos:
   - Clique em **Permitir acesso de convidado a programas da rede gerenciada** para conceder ao computador acesso à rede (você pode usar essa opção para usuários temporários em sua casa).
   - Clique em **Permitir acesso completo a programas da rede gerenciada** para conceder ao computador acesso à rede.

- Clique em **Permitir acesso administrativo a programas da rede gerenciada** para conceder ao computador acesso à rede com permissões administrativas. Isso também permite que o computador conceda acesso a outros computadores que desejem associar-se à rede gerenciada.

4. Clique em **OK**.
   Um convite para se associar à rede gerenciada é enviado para o computador. Quando o computador aceita o convite, duas cartas de baralho são exibidas.
5. Confirme se as cartas são as mesmas que estão sendo exibidas no computador que você convidou a se associar à rede gerenciada.
6. Clique em **Conceder acesso**.

Observação: Se o computador que convidou você para associar-se à rede gerenciada não estiver exibindo as mesmas cartas de baralho exibidas na caixa de diálogo de confirmação de segurança, houve uma violação na segurança da rede gerenciada. Permitir que o computador se associe à rede poderia colocar outros computadores em risco; portanto, clique em **Rejeitar acesso** na caixa de diálogo de confirmação de segurança.

Parar de confiar nos computadores da rede

Se confiar em outros computadores da rede por engano, você poderá deixar de confiar neles.

- Clique em **Parar de confiar nos computadores desta rede** em **Desejo**.

Observação: O link **Parar de confiar nos computadores desta rede** não estará disponível se você tiver permissões administrativas e houver outros computadores gerenciados na rede.

CAPÍTULO 27

Gerenciando a rede remotamente

Depois de configurar sua rede gerenciada, você pode gerenciar remotamente os computadores e componentes que fazem parte da rede. É possível gerenciar o status e os níveis de permissão dos computadores e componentes e corrigir a maioria das vulnerabilidades de segurança remotamente.

Neste capítulo

Monitorando status e permissões

Uma rede gerenciada possui membros gerenciados e não gerenciados. Membros gerenciados permitem que outros computadores da rede monitores seu status de proteção McAfee, enquanto membros não gerenciados não o permitem. Membros não gerenciados normalmente são computadores convidados que desejam acessar outros recursos da rede (enviar arquivos ou compartilhar impressoras, por exemplo). A qualquer momento, um computador não gerenciado pode ser convidado por outro membro gerenciado da rede a tornar-se membro gerenciado. Da mesma forma, um computador gerenciado pode tornar-se não gerenciado a qualquer momento.

Os computadores gerenciados possuem permissões de convidado, total ou administrativa. Permissões administrativas permitem que o computador gerenciado controle o status de proteção de todos os outros computadores gerenciados da rede, além de permitir que outros computadores se associem à rede. Permissões totais e de convidado permitem apenas que um computador acesse a rede. Você pode modificar o nível de permissão de um computador a qualquer momento.

Como uma rede gerenciada também é formada por dispositivos (como roteadores), você pode usar o Network Manager para gerenciá-los. Você também pode configurar e modificar as propriedades de exibição de um dispositivo no mapa da rede.

Monitorar o status de proteção de um computador

Se o status de proteção de um computador não estiver sendo monitorado na rede (se o computador não for um membro ou se ele for um computador não gerenciado), você poderá solicitar o monitoramento.

1 Clique no ícone correspondente a um computador não gerenciado no mapa de rede.
2 Clique em **Monitorar este computador**, em **Desejo**.

Parar de monitorar o status de proteção de um computador

É possível parar de monitorar o status de proteção de um computador gerenciado na rede; contudo, ele se tornará um computador não gerenciado e você não poderá monitorar seus status de proteção remotamente.

1 Clique no ícone correspondente a um computador gerenciado no mapa de rede.
2 Clique em **Parar a monitoração deste computador**, em **Desejo**.
3 Na caixa de diálogo de confirmação, clique em **Sim**.

Modificar as permissões de um computador gerenciado

Você pode alterar as permissões de um computador gerenciado a qualquer momento. Isso permite que você modifique os computadores que podem monitorar o status de proteção de outros computadores da rede.

1. Clique no ícone correspondente a um computador gerenciado no mapa de rede.
2. Clique em **Modificar permissões para este computador**, em **Desejo**.
3. Na caixa de diálogo de modificação de permissões, marque ou desmarque a caixa de seleção para determinar se este e outros computadores da rede gerenciada podem monitorar o status de proteção uns dos outros.
4. Clique em **OK**.

Gerenciar um dispositivo

Você pode gerenciar um dispositivo acessando sua página de administração na Web a partir do Network Manager.

1. Clique no ícone de um dispositivo no mapa de rede.
2. Clique em **Gerenciar este dispositivo**, em **Desejo**.
   Um navegador da Web será aberto e exibirá a página da Web de administração do dispositivo.
3. Em seu navegador da Web, forneça suas informações de login e defina as configurações de segurança do dispositivo.

Observação: Se o dispositivo for um ponto de acesso ou roteador sem fio protegido pelo Wireless Network Security, você deve usar o Wireless Network Security para definir suas configurações de segurança.

Modificar as propriedades de exibição de um dispositivo

Quando modifica as propriedades de exibição de um dispositivo, você pode mudar o nome de exibição dele no mapa de rede e especificar se ele é um roteador sem fio.

1. Clique no ícone de um dispositivo no mapa de rede.
2. Clique em **Modificar propriedades de dispositivo**, em **Desejo**.
3. Para especificar o nome de exibição do dispositivo, digite um nome na caixa **Nome**.
4. Para especificar o tipo de dispositivo, clique em **Roteador padrão**, se ele não for um roteador sem fio, ou em **Roteador sem fio**.
5. Clique em **OK**.

Corrigindo vulnerabilidades de segurança

Computadores gerenciados com permissões administrativas podem monitorar o status de proteção McAfee de outros computadores gerenciados na rede e corrigir remotamente os problemas de vulnerabilidade da segurança relatados. Por exemplo, se o status de proteção McAfee de um computador gerenciado indicar que o VirusScan está desativado, outro computador gerenciado com permissões administrativas poderá ativar o VirusScan remotamente.

Quando vulnerabilidades de segurança são corrigidas remotamente, o Network Manager repara a maioria dos problemas relatados. No entanto, algumas vulnerabilidades podem exigir intervenção manual no computador local. Nesse caso, o Network Manager corrige os problemas que podem ser reparados remotamente e solicita que você corrija os problemas restantes efetuando logon no SecurityCenter no computador vulnerável e seguindo as recomendações fornecidas. Em alguns casos, a solução sugerida é a instalação da versão mais recente do SecurityCenter em um ou mais computadores remotos da rede.

Corrigir vulnerabilidades de segurança

Você pode usar o Network Manager para corrigir a maioria das vulnerabilidades de segurança em computadores remotos gerenciados. Por exemplo, se o VirusScan estiver desativado em um computador remoto, você poderá ativá-lo.

1. Clique no ícone do item no mapa de rede.
2. Exiba o status de proteção do item em **Detalhes**.
3. Clique em **Corrigir vulnerabilidades de segurança** em **Desejo**.
4. Quando os problemas de segurança estiverem corrigidos, clique em **OK**.

Observação: Embora o Network Manager corrija automaticamente a maioria das vulnerabilidades de segurança, alguns reparos exigem que você abra o SecurityCenter no computador vulnerável e siga as recomendações fornecidas.

Instalar software de segurança McAfee em computadores remotos

Se um ou mais computadores da sua rede não estiverem usando a versão mais recente do SecurityCenter, os respectivos status de proteção não poderão ser monitorados remotamente. Se quiser monitorar esses computadores remotamente, instale a versão mais recente do SecurityCenter em cada um deles.

1. Abra o SecurityCenter no computador em que você deseja instalar o software.
2. Em **Tarefas comuns**, clique em **Minha conta**.
3. Efetue logon usando o endereço de e-mail e a senha utilizados para registrar o software de segurança na primeira instalação.
4. Selecione o produto apropriado, clique no ícone **Fazer download/Instalar** e siga as instruções na tela.

C A P Í T U L O 28

McAfee EasyNetwork

O EasyNetwork permite que você compartilhe arquivos com segurança, simplifique as transferências de arquivos e compartilhe impressoras entre computadores de sua rede doméstica. Contudo, os computadores de sua rede devem ter o EasyNetwork instalado para acessar seus recursos.

Antes de usar o EasyNetwork, você pode se familiarizar com alguns dos recursos. A Ajuda do Easynetwork fornece detalhes sobre como configurar e usar esses recursos.

Observação: O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician.

Neste capítulo

Recursos do EasyNetwork

O EasyNetwork fornece os recursos a seguir.

Compartilhamento de arquivos

O EasyNetwork facilita o compartilhamento de arquivos com outros computadores de sua rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura a esses arquivos. Apenas os computadores com acesso administrativo ou total à rede gerenciada (membros) podem compartilhar ou acessar arquivos compartilhados por outros membros.

Transferência de arquivos

Você pode enviar arquivos para outros computadores com acesso administrativo ou total à sua rede gerenciada (membros). Quando você recebe um arquivo, ele aparece em sua caixa de entrada do EasyNetwork. A caixa de entrada é um local de armazenamento temporário para todos os arquivos enviados para você por outros computadores da rede.

Compartilhamento automático de impressoras

Depois que se associar à rede gerenciada, você poderá compartilhar com outros membros todas as impressoras locais conectadas ao seu computador, usando o nome atual da impressora como o nome da impressora compartilhada. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e use essas impressoras.

CAPÍTULO 29

Configurando o EasyNetwork

Antes de usar o EasyNetwork, você terá que abri-lo e se associar a uma rede gerenciada. Depois de se associar a uma rede gerenciada, você poderá compartilhar, pesquisar e enviar arquivos para outros computadores da rede. Também é possível compartilhar impressoras. Você poderá sair da rede a qualquer momento, se desejar.

Neste capítulo

Abrir o EasyNetwork

Por padrão, você é solicitado a abrir o EasyNetwork depois de sua instalação, mas também é possível abri-lo mais tarde.

- No menu **Iniciar**, aponte para **Programas**, aponte para **McAfee** e clique em **McAfee EasyNetwork**.

Dica: Se criou ícones na área de trabalho e na inicialização rápida durante a instalação, você também poderá abrir o EasyNetwork clicando duas vezes no ícone do McAfee EasyNetwork na área de trabalho ou na área de notificação à direita da barra de tarefas.

Associando-se a uma rede gerenciada

Se nenhum computador da rede à qual você está conectado tiver o SecurityCenter, você se tornará um membro da rede e será solicitado a identificar se a rede é confiável. Por ser o primeiro computador a associar-se à rede, o nome do seu computador é incluído no nome da rede, mas você poderá renomeá-la quando desejar.

Quando um computador se conecta à rede, ele envia uma solicitação de associação para todos os outros computadores da rede. A solicitação pode ser concedida por qualquer outro computador com permissões administrativas da rede. O concessor também pode determinar o nível de permissão para o computador que está se associando à rede; por exemplo, convidado (apenas para transferência de arquivos) ou total/administrativa (transferência e compartilhamento de arquivos). No EasyNetwork, computadores com acesso administrativo podem conceder acesso a outros computadores e gerenciar permissões (promover ou rebaixar computadores); computadores com acesso total não podem executar essas tarefas administrativas.

Observação: Depois que se associar, se você tiver outros programas de rede da McAfee instalados (o Network Manager, por exemplo), o computador também será reconhecido como membro gerenciado nesses programas. O nível de permissão atribuído a um computador no EasyNetwork aplica-se a todos os programas de rede da McAfee. Para obter mais informações sobre o que significam permissões de convidado, total ou administrativa em outros programas de rede da McAfee, consulte a documentação fornecida com o programa.

Associar-se à rede

Quando um computador se conecta a uma rede confiável pela primeira vez depois da instalação do EasyNetwork, uma mensagem pergunta se você deseja se associar à rede gerenciada. Se o computador concorda em se associar, uma solicitação é enviada para todos os outros computadores da rede que têm acesso administrativo. Essa solicitação deve ser concedida para que o computador possa compartilhar impressoras e arquivos ou enviar e copiar arquivos da rede. O primeiro computador da rede recebe permissões administrativas automaticamente.

1. Na janela Arquivos compartilhados, clique em **Associar a essa rede**.
   Quando um computador administrador da rede autorizar sua solicitação, aparecerá uma mensagem perguntando se você deseja permitir que esse computador e os outros computadores da rede gerenciem as configurações de segurança uns dos outros.
2. Para permitir que seu computador e os outros da rede gerenciem as configurações de segurança uns dos outros, clique em **OK**; caso contrário, clique em **Cancelar**.
3. Confirme se o computador concessor exibe as mesmas cartas de baralho exibidas na caixa de diálogo de confirmação de segurança e clique em **OK**.

Observação: Se o computador que convidou você para associar-se à rede gerenciada não estiver exibindo as mesmas cartas de baralho exibidas na caixa de diálogo de confirmação de segurança, houve uma violação na segurança da rede gerenciada. Associar-se à rede poderia colocar seu computador em risco; por isso, clique em **Cancelar** na caixa de diálogo de confirmação de segurança.

Conceder acesso à rede

Quando um computador solicita associação à rede gerenciada, uma mensagem é enviada aos outros computadores da rede que têm acesso administrativo. O primeiro computador a responder se torna o concessor. Como concessor, você é responsável por decidir que tipo de acesso deve ser concedido ao computador: convidado, total ou administrativo.

1. No alerta, clique no nível de acesso apropriado.
2. Na caixa de diálogo Convidar um computador para associar-se à rede gerenciada, execute um dos seguintes procedimentos:
   - Clique em **Permitir acesso de convidado a programas da rede gerenciada** para conceder ao computador acesso à rede (você pode usar essa opção para usuários temporários em sua casa).

- Clique em **Permitir acesso completo a programas da rede gerenciada** para conceder ao computador acesso à rede.
- Clique em **Permitir acesso administrativo a programas da rede gerenciada** para conceder ao computador acesso à rede com permissões administrativas. Isso também permite que o computador conceda acesso a outros computadores que desejem associar-se à rede gerenciada.

3 Clique em **OK**.

4 Confirme se o computador concessor está exibindo as mesmas cartas de baralho exibidas na caixa de diálogo de confirmação de segurança e clique em **Conceder acesso**.

Observação: Se o computador não exibir as mesmas cartas que estão sendo exibidas na caixa de diálogo de confirmação de segurança, houve uma violação de segurança na rede gerenciada. Conceder acesso à rede para esse computador pode colocar seu computador em risco; portanto, clique em **Rejeitar acesso** na caixa de diálogo de confirmação de segurança.

Renomear a rede

Por padrão, o nome da rede inclui o nome do primeiro computador associado, mas você pode mudar o nome da rede a qualquer momento. Ao renomear a rede, você muda a descrição dela exibida no EasyNetwork.

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, digite o nome da rede na caixa **Nome da rede**.
3. Clique em **OK**.

Saindo de uma rede gerenciada

Caso se associe a uma rede gerenciada e depois decida que não quer mais ser um membro dela, você poderá deixar a rede. Depois de deixar a rede gerenciada, você poderá se associar novamente, mas terá que receber permissão de novo. Para obter mais informações sobre associação, consulte Associando-se a uma rede gerenciada (página 162).

Sair de uma rede gerenciada

Você pode sair da rede gerenciada à qual se associou anteriormente.

1 No menu **Ferramentas**, clique em **Sair da rede**.

2 Na caixa de diálogo Sair da rede, selecione o nome da rede da qual deseja sair.

3 Clique em **Sair da rede**.

CAPÍTULO 30

Compartilhando e enviando arquivos

O EasyNetwork facilita o compartilhamento e o envio de arquivos entre outros computadores da rede. Ao compartilhar arquivos, você concede aos outros computadores acesso somente leitura. Apenas computadores membros da rede gerenciada (acesso total ou administrativo) podem compartilhar ou acessar arquivos compartilhados por outros computadores-membros.

Observação: Se estiver compartilhando um grande número de arquivos, os recursos do seu computador podem ser afetados.

Neste capítulo

Compartilhando arquivos

Apenas computadores membros da rede gerenciada (acesso total ou administrativo) podem compartilhar ou acessar arquivos compartilhados por outros computadores-membros. Se você compartilhar uma pasta, todos os arquivos da pasta e suas subpastas serão compartilhados, mas arquivos adicionados posteriormente à pasta não serão compartilhados automaticamente. Se uma pasta ou um arquivo compartilhado for excluído, será removido da janela Arquivos compartilhados. É possível parar de compartilhar arquivos a qualquer momento.

Para acessar um arquivo compartilhado, abra o arquivo diretamente pelo EasyNetwork ou copie-o para o seu computador e, em seguida, abra-o localmente. Você poderá procurar arquivos compartilhados, se a sua lista de arquivos compartilhados for grande e dificultar a localização do arquivo.

Observação: Os arquivos compartilhados com o EasyNetwork não podem ser acessados de outros computadores pelo Windows Explorer, porque o compartilhamento de arquivos do EasyNetwork deve ser realizado por conexões seguras.

Compartilhar um arquivo

Quando você compartilha um arquivo, ele se torna disponível para todos os membros com acesso total ou administrativo à rede gerenciada.

1. No Windows Explorer, localize o arquivo que deseja compartilhar.
2. Arraste o arquivo de seu local no Windows Explorer até a janela Arquivos compartilhados no EasyNetwork.

Dica: Você também pode compartilhar um arquivo, se clicar em **Compartilhar arquivos**, no menu **Ferramentas**. Na caixa de diálogo Compartilhar, navegue até a pasta em que está armazenado o arquivo que você deseja compartilhar, selecione-o e clique em **Compartilhar**.

Parar de compartilhar um arquivo

Se você compartilhar um arquivo na rede gerenciada, poderá parar de compartilhá-lo a qualquer momento. Quando você pára de compartilhar um arquivo, os outros membros da rede gerenciada não podem mais acessá-lo.

1. No menu **Ferramentas**, clique em **Deixar de compartilhar arquivos**.
2. Na caixa de diálogo Deixar de compartilhar arquivos, selecione o arquivo que não deseja mais compartilhar.
3. Clique em **OK**.

Copiar um arquivo compartilhado

Copie um arquivo compartilhado para poder acessá-lo mesmo que ele não esteja mais compartilhado. Você pode copiar um arquivo compartilhado de qualquer computador da rede gerenciada.

- Arraste um arquivo da janela Arquivos compartilhados do EasyNetwork para um local no Windows Explorer ou para a área de trabalho do Windows.

Dica: Você também pode copiar um arquivo compartilhado, se selecioná-lo no EasyNetwork e, em seguida, clicar em **Copiar para**, no menu **Ferramentas**. Na caixa de diálogo Copiar para, navegue até a pasta para a qual deseja copiar o arquivo, selecione-a e clique em **Salvar**.

Procurar um arquivo compartilhado

Você pode procurar um arquivo que foi compartilhado por você ou por qualquer outro membro da rede. Enquanto você digita os critérios de pesquisa, o EasyNetwork exibe os resultados correspondentes na janela Arquivos compartilhados.

1. Na janela Arquivos compartilhados, clique em **Pesquisar**.
2. Clique na opção apropriada (página 169), na lista **Contém**.
3. Digite uma parte ou todo o nome do arquivo ou caminho na lista **Nome do arquivo ou caminho**.
4. Clique no tipo de arquivo (página 169) apropriado, na lista **Tipo**.
5. Nas listas **De** e **Até**, clique nas datas que representam o intervalo de datas em que o arquivo foi criado.

Critérios de pesquisa

As tabelas a seguir descrevem os critérios de pesquisa que você pode especificar quando pesquisar arquivos compartilhados.

Nome do arquivo ou do caminho

Contém	Descrição
Contém todas as palavras	Pesquisa nomes de arquivos ou de caminhos que contenham todas as palavras especificadas na lista **Nome do arquivo ou caminho**, em qualquer ordem.
Contém qualquer uma das palavras	Pesquisa um nome de arquivo ou de caminho que contenha qualquer uma das palavras especificadas na lista **Nome do arquivo ou caminho**.

Contém	Descrição
Contém a seqüência de caracteres exata	Pesquisa um nome de arquivo ou de caminho que contenha a frase exata especificada na lista **Nome do arquivo ou caminho**.

Tipo de arquivo

Tipo	Descrição
Qualquer	Pesquisa todos os tipos de arquivos compartilhados.
Documento	Pesquisa todos os documentos compartilhados.
Imagem	Pesquisa todos os arquivos de imagem compartilhados.
Vídeo	Pesquisa todos os arquivos de vídeo compartilhados.
Áudio	Pesquisa todos os arquivos de áudio compartilhados.
Compactado	Pesquisa todos os arquivos compactados (arquivos .zip, por exemplo).

Enviando arquivos para outros computadores

É possível enviar arquivos a outros computadores que sejam membros da rede gerenciada. Antes de enviar um arquivo, o EasyNetwork confirma se o computador de destino tem espaço em disco disponível suficiente.

Quando você recebe um arquivo, ele aparece em sua caixa de entrada do EasyNetwork. A caixa de entrada é um local de armazenamento temporário para os arquivos enviados para você por outros computadores da rede. Se o EasyNetwork estiver aberto no momento em que você receber um arquivo, o arquivo aparecerá instantaneamente em sua caixa de entrada. Caso contrário, aparecerá uma mensagem na área de notificação à direita da barra de tarefas. Se não quiser receber mensagens de notificação (porque elas interrompem o que você está fazendo, por exemplo), você poderá desativar esse recurso. Se um arquivo com o mesmo nome já existir na caixa de entrada, o novo arquivo é renomeado com um sufixo numérico. Os arquivos continuam em sua caixa de entrada até que você os aceite (copiando-os em seu computador).

Enviar um arquivo para outro computador

Você pode enviar um arquivo para outro computador na rede gerenciada sem compartilhá-lo. Para que um usuário no computador de destino possa exibir o arquivo, ele deve ser salvo localmente. Para obter mais informações, consulte Aceitar um arquivo de outro computador (página 172).

1 No Windows Explorer, localize o arquivo que deseja enviar.

2 Arraste o arquivo de seu local no Windows Explorer até um ícone de um computador ativo no EasyNetwork.

Dica: Para enviar diversos arquivos para um computador, pressione CTRL ao selecionar os arquivos. Também é possível enviar os arquivos, se você clicar em **Enviar**, no menu **Ferramentas**, selecionar os arquivos e, em seguida, clicar em **Enviar**.

Aceitar um arquivo de outro computador

Se outro computador da rede gerenciada enviar um arquivo para você, você deverá aceitá-lo, salvando-o em seu computador. Se o EasyNetwork não estiver em execução quando um arquivo for enviado para o seu computador, você receberá uma mensagem de notificação, na área de notificação, à direita da barra de tarefas. Clique na mensagem de notificação para abrir o EasyNetwork e acessar o arquivo.

- Clique em **Recebido** e arraste o arquivo da caixa de entrada do EasyNetwork para uma pasta no Windows Explorer.

Dica: Você também pode receber um arquivo de outro computador, se você selecionar o arquivo na caixa de entrada do EasyNetwork e clicar em **Aceitar**, no menu **Ferramentas**. Na caixa de diálogo Aceitar, navegue até a pasta em que deseja salvar os arquivos recebidos, selecione-a e clique em **Salvar**.

Receber uma notificação quando um arquivo for enviado

É possível receber uma mensagem de notificação quando outro computador da rede gerenciada enviar um arquivo. Se o EasyNetwork não estivem em execução, a mensagem de notificação será exibida na área de notificação à extrema direita da barra de tarefas.

1. No menu **Opções**, clique em **Configurar**.
2. Na caixa de diálogo Configurar, marque a caixa de seleção **Notificar quando outro computador enviar arquivos para mim**.
3. Clique em **OK**.

CAPÍTULO 31

Compartilhando impressoras

Depois que você se associa à rede gerenciada, o EasyNetwork compartilha as impressoras locais conectadas ao seu computador e usa o nome da impressora como nome da impressora compartilhada. Ele também detecta impressoras compartilhadas por outros computadores em sua rede e permite que você configure e as use.

Se você tiver configurado um driver de impressora para imprimir através de um servidor de impressão da rede (por exemplo, um servidor de impressão USB sem fio), o EasyNetwork considerará essa impressora como uma impressora local e a compartilhará na rede. Também é possível parar de compartilhar uma impressora a qualquer momento.

Neste capítulo

Trabalhando com impressoras compartilhadas

O EasyNetwork detecta as impressoras compartilhadas pelos computadores na rede. Se o EasyNetwork detectar uma impressora remota que não esteja conectada ao seu computador, o link **Impressoras de rede disponíveis** aparecerá na janela Arquivos compartilhados quando você abrir o EasyNetwork pela primeira vez. Em seguida, você poderá instalar as impressoras disponíveis ou desinstalar as impressoras que já estão conectadas ao seu computador. Você também pode atualizar a lista de impressoras para garantir que está exibindo informações atualizadas.

Se você ainda não se associou à rede gerenciada, mas está conectado a ela, é possível acessar as impressoras compartilhadas a partir do painel de controle do Windows.

Parar de compartilhar uma impressora

Quando você parar de compartilhar uma impressora, os membros não poderão mais usá-la.

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Gerenciar impressoras da rede, clique no nome da impressora que não deseja mais compartilhar.
3. Clique em **Não compartilhar**.

Instalar uma impressora de rede disponível

Se for um membro da rede gerenciada, você pode acessar as impressoras compartilhadas. Contudo, você deverá instalar o driver usado pela impressora. Se o proprietário da impressora parar de compartilhá-la, você não poderá mais usá-la.

1. No menu **Ferramentas**, clique em **Impressoras**.
2. Na caixa de diálogo Impressoras de rede disponíveis, clique em um nome de impressora.
3. Clique em **Instalar**.

Referência

O Glossário de termos lista e define a terminologia de segurança usada com mais freqüência nos produtos McAfee.

Glossário

8

802.11

Um conjunto de padrões IEEE para transmitir dados através de uma rede sem fio. O 802.11 é conhecido como Wi-Fi.

802.11a

Uma extensão do 802.11 que transmite dados a até 54 Mbps na banda de 5 GHz. Embora a velocidade de transmissão seja maior do que com o 802.11b, o alcance é muito menor.

802.11b

Uma extensão do 802.11 que transmite dados a até 11 Mbps na banda de 2,4 GHz. Embora a velocidade de transmissão seja menor do que a do 802.11a, o alcance é muito maior.

802.1x

Um padrão IEEE para autenticação em redes com ou sem fio. O 802.1x normalmente é usado com redes sem fio 802.11.

A

adaptador sem fio

Um dispositivo que adiciona recurso sem fio a um computador ou PDA. É conectado por uma porta USB, slot de PC Card (CardBus), slot de placa de memória ou internamente no barramento PCI.

arquivamento completo

Para arquivar um conjunto completo de dados com base nos tipos de arquivos e locais que você configurou. Consulte também arquivamento rápido.

arquivamento rápido

Arquivar apenas os arquivos que foram alterados desde o último arquivamento rápido ou completo. Consulte também arquivamento completo.

arquivar

Criar uma cópia de arquivos importantes na unidade USB, de CD, de DVD, de disco rígido externo ou de rede.

arquivo temporário

Um arquivo, criado na memória ou no disco, pelo sistema operacional ou por algum outro programa, para ser usado durante uma sessão e descartado em seguida.

atalho

Um arquivo que contém somente o local de outro arquivo no computador.

ataque de dicionário

Um tipo de ataque de força bruta que usa palavras comuns para tentar descobrir uma senha.

ataque de força bruta

Um método para decodificar dados criptografados, como senhas, através de procedimentos exaustivos (ou seja, força bruta) em vez de empregar estratégias intelectuais. A força bruta é considerada um método de ataque infalível, embora demorado. O ataque de força bruta também é chamado de cracking por força bruta.

ataque man-in-the-middle (homem no meio)

Um método de interceptação e possível modificação de mensagens entre duas partes, sem que nenhuma delas saiba que o link de comunicação foi violado.

autenticação

O processo de identificação de um indivíduo, normalmente com base em um nome de usuário e uma senha exclusivos.

B

backup

Criar uma cópia de arquivos importantes em um servidor on-line seguro.

biblioteca

Uma área de armazenamento on-line para os arquivos submetidos ao backup e publicados. A biblioteca do Data Backup é um site na Internet, que pode ser acessado por qualquer pessoa que tenha acesso à Internet.

C

cache

Uma área de armazenamento temporário em seu computador. Por exemplo, para aumentar a velocidade e a eficiência da navegação na Internet, seu navegador poderá recuperar uma página da Web do respectivo cache (em vez de recuperá-la de um servidor remoto) na próxima vez que você quiser visualizá-la.

cavalo de Tróia

Um programa que parece legítimo, mas que pode danificar arquivos importantes, comprometer o desempenho e permitir acesso não autorizado ao seu computador.

chave

Vários números e letras usados por dois dispositivos para autenticar sua comunicação. Ambos os dispositivos precisam ter a chave. Consulte também WEP, WPA, WPA2, WPA-PSK e WPA2-PSK.

cliente

Um aplicativo, executado em um computador pessoal ou estação de trabalho, que depende de um servidor para executar algumas operações. Por exemplo, um cliente de e-mail é um aplicativo que permite a você enviar e receber e-mail.

cliente de e-mail

Um programa que você executa em seu computador para enviar e receber e-mails (o Microsoft Outlook, por exemplo).

Cofre de senhas

Uma área de armazenamento segura para suas senhas pessoais. Ele permite que você guarde suas senhas, garantindo que nenhum outro usuário (nem mesmo um administrador) poderá acessá-las.

compactação

Um processo através do qual os arquivos são compactados em um formato que minimiza o espaço necessário para armazená-los ou transmiti-los.

compartilhar

Permitir que os destinatários de e-mail acessem os arquivos com backup selecionados, por um período limitado. Ao compartilhar um arquivo, você envia a cópia de backup do arquivo para os destinatários de e-mail especificados. Os destinatários recebem uma mensagem de e-mail do Data Backup, indicando que os arquivos foram compartilhados com eles. O e-mail também contém um link para os arquivos compartilhados.

conta de e-mail padrão

Consulte POP3.

Controle ActiveX

Um componente de software usado por programas ou páginas da Web para adicionar funcionalidades que são exibidas como uma parte normal do programa ou da página da Web. A maioria dos controles ActiveX é inofensiva, porém, alguns deles podem capturar informações do seu computador.

Controles pelos pais

Configurações que ajudam a controlar o que seus filhos vêem e fazem enquanto navegam na Internet. Para configurar os Controles pelos pais, você pode ativar ou desativar a filtragem de imagens, escolher um grupo de classificação de conteúdo e definir limites de horário para navegação na Web.

cookie

Um pequeno arquivo que contém informações que geralmente incluem um nome de usuário e a data e a hora atuais, e é armazenado no computador de uma pessoa que está navegando na Internet. Os cookies são usados principalmente por sites para identificar os usuários que se registraram no site ou que o visitaram anteriormente. Contudo, eles também podem ser uma fonte de informação para hackers.

criptografia

Um processo através do qual os dados são transformados de texto para código, ocultando as informações para que fiquem ilegíveis para as pessoas que não sabem descriptografá-las. Os dados criptografados também são conhecidos como texto codificado.

D

DAT

(Data signature files, Arquivos de assinatura de dados) Arquivos que contêm as definições usadas no momento da detecção de vírus, cavalos de Tróia, spyware, adware e outros programas possivelmente indesejados em seu computador ou na unidade USB.

discador

Software que ajuda você a estabelecer uma conexão com a Internet. Quando usados de forma maliciosa, os discadores podem redirecionar suas conexões da Internet para um provedor diferente do seu Provedor de serviços de Internet (ISP) padrão, sem informar sobre os custos adicionais.

disco rígido externo

Uma unidade de disco rígido que é armazenada fora do computador.

DNS

(Domain Name System, Sistema de nomes de domínios) Um sistema que converte nomes de host ou nomes de domínio em endereços IP. Na Internet, o DNS é usado para converter endereços da Web de fácil leitura (por exemplo, www.meunomedehost.com) em endereços IP (por exemplo, 111.2.3.44), para que o site possa ser recuperado. Sem o DNS, você precisaria digitar o endereço IP no navegador.

domínio

Um descritor ou uma sub-rede local para sites na Internet.

Em uma LAN (rede local), um domínio é uma sub-rede composta de computadores servidores e clientes, controlados por um banco de dados de segurança. Neste contexto, os domínios podem melhorar o desempenho. Na Internet, um domínio é parte de todos os endereços da Web (por exemplo, em www.abc.com, abc é o domínio).

E

e-mail

(correio eletrônico) Mensagens enviadas e recebidas eletronicamente, através de uma rede de computadores. Consulte também Webmail.

Endereço IP

Um identificador para um computador ou dispositivo em uma rede TCP/IP. As redes que usam o protocolo TCP/IP roteiam as mensagens com base no endereço IP de destino. O formato de um endereço IP consiste em uma seqüência numérica de 32 bits escritos como quatro números separados por pontos. Cada número pode estar entre 0 e 255 (por exemplo, 192.168.1.100).

Endereço MAC

(Media Access Control, Controle de acesso de mídia) Um número de série exclusivo atribuído a um dispositivo físico, que está acessando a rede.

ESS

(Extended Service Set, Conjunto de serviços estendido) Um conjunto de duas ou mais redes que formam uma única sub-rede.

estação

Um único computador conectado a uma rede.

evento

Uma ação iniciada pelo usuário, pelo dispositivo ou pelo próprio computador que aciona uma resposta. O McAfee registra eventos seu registro de eventos.

F

falsificação de IP

Consiste em forjar o endereço IP de um pacote IP. Isso é usado em diversos tipos de ataque, incluindo seqüestro de sessão. Também é freqüentemente utilizado para falsificar os cabeçalhos de e-mail de SPAM para impedir que sejam rastreados corretamente.

filtragem de imagens

Uma opção do Controle pelos pais que bloqueia a exibição de imagens da Web potencialmente inadequadas.

firewall

Um sistema (hardware, software ou ambos) desenvolvido para impedir o acesso não autorizado a uma rede privada ou a partir de uma rede privada. Firewalls são freqüentemente utilizados para impedir usuários da Internet não autorizados de acessarem redes privadas conectadas à Internet, especialmente intranets. Todas as mensagens que entram ou saem da intranet passam pelo firewall, que examina cada uma delas e bloqueia as que não atendem aos critérios de segurança especificados.

fragmentos de arquivo

Vestígios de um arquivo espalhados por um disco. A fragmentação de arquivo ocorre quando arquivos são adicionados ou excluídos e pode prejudicar o desempenho do computador.

gateway integrado

Um dispositivo que combina as funções de um ponto de acesso (PA), roteador e firewall. Alguns dispositivos também podem incluir aperfeiçoamentos de segurança e recursos de ponte.

grupo de classificação de conteúdo

Em Controles pelos pais, o grupo de faixa etária ao qual o usuário pertence. O conteúdo é disponibilizado ou bloqueado com base no grupo de classificação de conteúdo ao qual o usuário pertence. Os grupos de classificação de conteúdo incluem: Crianças pequenas, crianças, pré-adolescentes, adolescentes e adultos.

H

hotspot

Uma região geográfica coberta por um ponto de acesso (PA) Wi-Fi (802.11). Os usuários que entram em um hotspot com um laptop sem fio podem se conectar à Internet, desde que o hotspot esteja enviando beacons (ou seja, anunciando sua presença) e não seja necessária autenticação. Os hotspots geralmente estão localizados em áreas com alta concentração de pessoas, como aeroportos.

I

Internet

A Internet é composta por um grande número de redes interconectadas que usam protocolos TCP/IP para a localização e a transferência de dados. A Internet surgiu como uma rede criada para ligar computadores de universidades e faculdades (no fim da década de 60 e começo de 70), fundada pelo Departamento de Defesa dos EUA e era chamada ARPANET. A Internet hoje é uma rede global de quase 100.000 redes independentes.

intranet

Uma rede de computadores privada, que normalmente pertence a uma organização e só pode ser acessada por usuários autorizados.

L

LAN

(Local Area Network, Rede local) Uma rede de computadores que abrange uma área relativamente pequena (como a de um único edifício, por exemplo). Computadores em uma LAN podem se comunicar uns com os outros e compartilhar recursos como impressoras e arquivos.

largura de banda

A quantidade de dados que podem ser transmitidos em um determinado período de tempo.

launchpad

Um componente de interface da U3 que funciona como um ponto de partida para iniciar e gerenciar programas USB U3.

lista branca

Uma lista de sites da Web que os usuários têm permissão para acessar, porque os sites não são considerados fraudulentos.

lista de confiáveis

Contém itens em que você confiou e não estão sendo detectados. Se confiar em um item (por exemplo, um programa potencialmente indesejado ou uma alteração de registro) por engano, ou se desejar que o item seja detectado novamente, você deverá removê-lo dessa lista.

lista negra

No anti-phishing, uma lista de sites da Web que são considerados fraudulentos.

Lixeira

Uma lixeira simulada para arquivos e pastas excluídas no Windows.

locais de observação

As pastas no seu computador monitoradas pelo Data Backup.

locais de observação superficial

Uma pasta em seu computador na qual as alterações são monitoradas pelo Data Backup. Se você configurar um local de observação superficial, o Data Backup fará backup dos tipos de arquivos em observação dentro dessa pasta, mas não incluirá suas subpastas.

local de observação detalhada

Uma pasta em seu computador na qual as alterações são monitoradas pelo Data Backup. Se você definir um local de observação detalhada, o Data Backup fará backup dos tipos de arquivos em observação dentro dessa pasta e de suas subpastas.

M

MAC (message authentication code, código de autenticação de mensagem)

Um código de segurança usado para criptografar mensagens transmitidas entre computadores. A mensagem é aceita se o computador reconhecer o código descriptografado como válido.

mapa de rede

Uma representação gráfica dos computadores e componentes que fazem parte de uma rede doméstica.

MAPI

(Messaging Application Programming Interface, Interface de programação de aplicativos de mensagens) Uma especificação de interface da Microsoft que permite a diferentes aplicativos de mensagens e de grupos de trabalho (incluindo e-mail, correio de voz ou fax) funcionar por meio de um único cliente, como o cliente Exchange.

MSN

(Microsoft Network) Um grupo de serviços baseados na Web oferecidos pela Microsoft Corporation, incluindo um mecanismo de pesquisa, e-mail, mensagens instantâneas e um portal.

N

navegador

Um programa usado para visualizar páginas da Web na Internet. Dois navegadores conhecidos são o Microsoft Internet Explorer e o Mozilla Firefox.

negação de serviço

Um tipo de ataque que reduz ou interrompe o tráfego em uma rede. Um ataque de negação de serviço (DoS, denial of service) ocorre quando uma rede é inundada com tantas solicitações adicionais que o tráfego regular fica lento ou é totalmente interrompido. Ele normalmente não resulta em roubo de informações ou outras vulnerabilidades de segurança.

NIC

(Network Interface Card, Placa de interface de rede) Uma placa que se conecta a um laptop ou a algum outro dispositivo e que conecta esse dispositivo à LAN.

P

palavra-chave

Um palavra que você pode atribuir a um arquivo com backup para estabelecer um relacionamento ou conexão com outros arquivos que possuam a mesma palavra-chave atribuída. Atribuir as palavras-chaves aos arquivos facilita a pesquisa pelos arquivos que você publicou na Internet.

phishing

Um golpe da Internet criado para obter informações valiosas (como números de cartão de crédito e de CPF, IDs de usuário e senhas) de indivíduos sem que eles saibam para usá-las de forma fraudulenta.

placa adaptadora sem fio USB

Uma placa adaptadora sem fio que é conectada a um slot USB no computador.

placas adaptadoras sem fio PCI

(Peripheral Component Interconnect, Interconexão de componente periférico) Uma placa adaptadora sem fio que se conecta a um slot de expansão PCI dentro do computador.

plug-in

Um pequeno programa que funciona com um programa maior para fornecer funções adicionais. Por exemplo, plug-ins permitem que o navegador da Web acesse e execute os arquivos incorporados nos documentos HTML que estejam em formatos que o navegador normalmente não reconheceria (por exemplo, animação, vídeo e arquivos de áudio).

Ponto de acesso

Um dispositivo de rede (geralmente chamado de roteador sem fio) que se conecta a um comutador ou hub Ethernet para ampliar o alcance físico do serviço para usuários sem fio. Quando os usuários sem fio se deslocam com seus dispositivos móveis, a transmissão passa de um ponto de acesso (PA) a outro para manter a conectividade.

ponto de acesso ilícito

Um Ponto de Acesso não autorizado. Os pontos de acesso ilícitos podem ser instalados em uma rede segura de empresa para conceder acesso de rede a terceiros não autorizados. Eles podem também ser criados para permitir que um invasor conduza um ataque man-in-the-middle.

ponto de restauração do sistema

Um instantâneo (imagem) do conteúdo da memória ou de um banco de dados do computador. O Windows cria pontos de restauração periodicamente e na hora em que ocorrem eventos significativos no sistema (como quando um programa ou driver é instalado). Você também pode criar e nomear seus próprios pontos de restauração a qualquer momento.

pop-ups

Pequenas janelas que aparecem sobre outras janelas na tela de seu computador. As janelas pop-up geralmente são usadas nos navegadores da Web para exibir anúncios.

POP3

(Post Office Protocol 3) Uma interface entre um programa cliente de e-mail e o servidor de e-mail. A maior parte dos usuários domésticos tem uma conta de e-mail POP3, também conhecida como conta de e-mail padrão.

porta

Um lugar por onde as informações entram e/ou saem de um computador. Por exemplo, um modem analógico convencional é conectado a uma porta serial.

PPPoE

(Point-to-Point Protocol Over Ethernet) Um método de usar o protocolo de discagem Point-to-Point Protocol (PPP) com Ethernet como o transporte.

programa potencialmente indesejado (PUP)

Um programa que coleta e transmite informações pessoais sem sua permissão (por exemplo, spyware e adware).

protocolo

Um formato (hardware ou software) para transmitir dados entre dois dispositivos. Seu computador ou dispositivo deverá oferecer suporte ao protocolo correto se você desejar se comunicar com outros computadores.

proxy

Um computador (ou software executado nele) que funciona como uma barreira entre uma rede e a Internet, apresentando somente um único endereço de rede para sites externos. Ao representar todos os computadores internos, o proxy protege identidades de rede ao mesmo tempo que oferece acesso à Internet. Consulte também servidor proxy.

publicar

Disponibilizar publicamente um arquivo com backup, na Internet. Você pode acessar arquivos publicados pesquisando a biblioteca do Data Backup.

Q

quarentena

Isolar. Por exemplo, no VirusScan, os arquivos suspeitos são detectados e colocados em quarentena para que eles não possam causar dano ao computador nem aos arquivos.

R

RADIUS

(Remote Access Dial-In User Service) Um protocolo que permite autenticação de usuário, normalmente numa situação de acesso remoto. Originalmente definido para uso com servidores de acesso remoto discado, o protocolo RADIUS é atualmente usado em uma variedade de ambientes de autenticação, incluindo a autenticação 802.1x do segredo compartilhado do usuário de uma WLAN.

rede

Uma coleção de pontos de acesso e seus usuários associados, equivalente a um ESS.

rede doméstica

Dois ou mais computadores conectados em uma residência, para que possam compartilhar arquivos e o acesso à Internet. Consulte também LAN.

rede gerenciada

Uma rede doméstica gerenciada com dois tipos de membros: membros gerenciados e não gerenciados. Membros gerenciados permitem que outros computadores da rede monitorem seus status de proteção, ao contrário dos membros não gerenciados.

registro

Um banco de dados em que o Windows armazena suas informações de configuração. O Registro contém perfis para cada usuário do computador e informações sobre as configurações de propriedade, os programas instalados e o hardware do sistema. O Windows sempre consulta essas informações durante seu funcionamento.

repositório de backup on-line

O local no servidor on-line em que seus arquivos são armazenados depois de submetidos ao backup.

restaurar

Recuperar uma cópia de um arquivo a partir do arquivamento ou do repositório online de backup.

roaming

Passar da área de cobertura de um ponto de acesso (PA) para a área de outro sem interrupção do serviço ou perda de conectividade.

rootkit

Uma coleção de ferramentas (programas) que concedem a um usuário acesso de nível de administrador a um computador ou rede de computadores. Os rootkits podem incluir spyware e outros programas potencialmente indesejados que podem criar riscos adicionais de segurança ou de privacidade para os dados de seu computador e suas informações pessoais.

roteador

Um dispositivo de rede que encaminha pacotes de dados de uma rede para outra. Baseado em tabelas de roteamento internas, os roteadores lêem cada pacote de entrada e decidem como encaminhá-lo com base em qualquer combinação de endereço de origem e destino, bem como nas condições de tráfego atuais (por exemplo, carga, custos das linhas e linhas ruins). Às vezes, um roteador é chamado de Ponto de Acesso (PA).

S

script

Uma lista de comandos que podem ser executados automaticamente (isto é, sem interação de usuário). Ao contrário de programas, os scripts são geralmente armazenados em formato de texto simples e compilados cada vez que são executados. Macros e arquivos de lotes são também chamados scripts.

segredo compartilhado

Uma cadeia de caracteres ou chave (geralmente uma senha) que foi compartilhada entre duas partes que se comunicaram antes de iniciar a comunicação. Um segredo compartilhado é usado para proteger partes confidenciais das mensagens RADIUS.

senha

Um código (geralmente composto de letras e números) utilizado para obter acesso a um computador, programa ou site.

servidor

Um computador ou programa que aceita conexões de outros computadores ou programas e retorna respostas adequadas. Por exemplo, seu programa de e-mail se conecta a um servidor de e-mail toda vez que você envia ou recebe mensagens de e-mail.

servidor DNS

(Servidor do Sistema de nomes de domínios) Um computador que retorna o endereço IP associado a um nome de host ou de domínio. Consulte também DNS.

Servidor proxy

Um componente de firewall que gerencia o tráfego da Internet de e para uma rede local (LAN). Um servidor proxy pode melhorar o desempenho, oferecendo dados solicitados com freqüência, como uma página popular da Web, e pode filtrar e descartar solicitações que o proprietário não considera apropriadas, como solicitações de acesso não autorizado a arquivos patenteados.

sincronizar

Resolver as inconsistências entre os arquivos do backup e os armazenados em seu computador local. Os arquivos são sincronizados quando a versão do arquivo no repositório on-line de backup for mais recente que a versão do arquivo em outros computadores.

SMTP

(Simple Mail Transfer Protocol) Um protocolo TCP/IP para enviar mensagens de um computador a outro em uma rede. Esse protocolo é usado na Internet para rotear o e-mail.

sobrecarga de buffer

Uma condição que ocorre quando programas ou processos suspeitos tentam armazenar em um buffer (área de armazenamento temporário) de seu computador mais dados do que ele suporta. As sobrecargas de buffer corrompem ou sobrescrevem dados em buffers adjacentes.

SSID

(Service Set Identifier) Um token (chave secreta) que identifica uma rede Wi-Fi (802.11). O SSID é configurado pelo administrador de rede e deve ser fornecido pelos usuários que desejam se juntar à rede.

SSL

(Secure Sockets Layer) Um protocolo desenvolvido pela Netscape para transmissão de documentos privados na Internet. A SSL funciona utilizando uma chave pública para criptografar dados que é transferida através da conexão SSL. Os URLs que exigem uma conexão SSL iniciam com https, em vez de http.

SystemGuard

Os alertas da McAfee que detectam alterações não autorizadas em seu computador e notificam você quando elas ocorrem.

T

texto codificado

Texto criptografado. O texto codificado é ilegível até ser convertido em texto simples (ou seja, descriptografado).

texto simples

Texto que não está criptografado. Veja também criptografia.

tipos de arquivos observados

Os tipos de arquivos (por exemplo, .doc, .xls e assim por diante) que o Data Backup submete a backup ou arquiva dentro dos locais de observação.

TKIP

(Temporal Key Integrity Protocol) Um protocolo que trata das falhas na segurança de WEP, principalmente a reutilização de chaves de criptografia. O TKIP altera as chaves temporais a cada 10.000 pacotes, proporcionando um método de distribuição dinâmico que melhora significativamente a segurança da rede. O processo (de segurança) TKIP começa com uma chave temporal de 128 bits compartilhada entre clientes e pontos de acesso (PAs). O TKIP combina a chave temporal com o endereço MAC do cliente e, em seguida, adiciona um vetor de inicialização relativamente grande de 16 octetos para produzir a chave que criptografa os dados. Esse procedimento garante que cada estação utilize fluxos de chaves diferentes para criptografar os dados. O TKIP usa RC4 para realizar a criptografia.

U3

(Você: simples, inteligente, móvel) Uma plataforma para executar programas do Windows 2000 ou do Windows XP diretamente de uma unidade USB. A iniciativa U3 foi fundada em 2004 pela M-Systems e pela SanDisk e permite que os usuários executem programas U3 em um computador Windows sem instalar ou armazenar dados ou configurações no computador.

unidade de rede

Uma unidade de disco ou de fita que é conectada a um servidor em uma rede compartilhada por vários usuários. Às vezes, as unidades de rede são denominadas unidades remotas.

unidade inteligente

Consulte unidade USB.

unidade USB

Uma pequena unidade de memória que se conecta a uma porta USB do computador. Uma unidade USB funciona como uma pequena unidade de disco, facilitando a transferência de arquivos de um computador para outro.

URL

(Uniform Resource Locator) O formato padrão para endereços da Internet.

USB

(Universal Serial Bus) Uma interface de computador serial padronizada que permite que você anexe dispositivos periféricos, como teclados, joysticks e impressoras, ao computador.

varredura em tempo real

Fazer a varredura em arquivos e pastas para verificar se há vírus e outra atividade quando eles são acessados por você ou seu computador.

varredura sob demanda

Uma varredura que é iniciada sob demanda (isto é, quando você inicia a operação). Diferentemente da varredura em tempo real, varreduras sob demanda não são iniciadas automaticamente.

vírus

Programas que se replicam, podendo alterar seus arquivos ou dados. Muitas vezes, eles parecem ser provenientes de um remetente confiável ou ter conteúdo inofensivo.

VPN

(Virtual Private Network) Uma rede privada configurada dentro de uma rede pública de modo a aproveitar as facilidades de gerenciamento da rede pública. As VPNs são usadas por empresas para criar redes de longa distância (WANs) que se estendem por grandes áreas geográficas, para fornecer conexões de site a site para escritórios de filiais ou para permitir que usuários móveis disquem para as LANs da empresa.

wardriver

Uma pessoa que pesquisa redes Wi-Fi (802.11) dirigindo por cidades equipadas com um computador Wi-Fi e algum hardware ou software especial.

Web bugs

Arquivos gráficos pequenos que podem ser incorporados em suas páginas HTML e que permitem que uma origem não autorizada configure os cookies em seu computador. Esses cookies podem então transmitir as informações para a origem não autorizada. Os Web bugs também são denominados beacons da Web, marcas de pixel, GIFs de limpeza ou GIFs invisíveis.

Webmail

Mensagens enviadas e recebidas eletronicamente, pela Internet. Consulte também e-mail.

WEP

(Wired Equivalent Privacy) Um protocolo de criptografia e autenticação definido como parte do padrão Wi-Fi (802.11). Suas versões iniciais baseiam-se em codificadores RC4 e possuem vulnerabilidades significativas. A WEP tenta proporcionar segurança criptografando os dados através de ondas de rádio, para que eles estejam protegidos ao serem transmitidos de um ponto para outro. No entanto, descobriu-se que a WEP não é tão segura quanto se acreditava.

Wi-Fi

(Wireless Fidelity) Um termo usado pela Wi-Fi Alliance ao se referir a qualquer tipo de rede 802.11.

Wi-Fi Alliance

Uma organização composta pelos principais fornecedores de hardware e software sem fio. A Wi-Fi Alliance empenha-se para certificar todos os produtos baseados em 802.11 quanto à interoperabilidade e promover o termo Wi-Fi como o nome de marca em todos os mercados para qualquer produto de LAN sem fio baseada em 802.11. A organização atua como associação, laboratório de testes e agência reguladora para fornecedores que queiram promover o crescimento do setor.

Wi-Fi Certified

Ser testado e aprovado pela Wi-Fi Alliance. Os produtos Wi-Fi Certified são considerados interoperáveis, embora eles possam ser originários de fabricantes diferentes. Um usuário com um produto Wi-Fi Certified pode usar qualquer marca de Ponto de Acesso (PA) com qualquer outra marca de hardware cliente que também seja certificado.

WLAN

(Wireless Local Area Network) Uma rede local (LAN) que usa uma conexão sem fio. Uma WLAN que usa ondas de rádio de alta freqüência, em vez de fios, para permitir que os computadores se comuniquem uns com os outros.

worm

Um worm é um vírus que se replica automaticamente na memória ativa e que pode enviar cópias de si mesmo através de e-mail. Os worms replicam e consomem recursos do sistema, reduzindo o desempenho ou interrompendo as tarefas.

WPA

(Wi-Fi Protected Access) Um padrão de especificação que aumenta em muito o nível de proteção de dados e o controle de acesso para sistemas de LAN sem fio futuros e existentes. Desenvolvido para ser executado em hardware existente ou como uma atualização de software, o WPA é derivado do padrão IEEE 802.11i, sendo compatível com este. Quando instalado corretamente, proporciona aos usuários de LAN sem fio um elevado grau de garantia de que seus dados permaneçam protegidos e que apenas usuários de rede autorizados tenham acesso à rede.

WPA-PSK

Um modo especial de WPA desenvolvido para usuários domiciliares que não precisam de uma segurança tão forte quanto a de empresas e que não têm acesso a servidores de autenticação. Nesse modo, o usuário doméstico digita manualmente a senha inicial para ativar o Wi-Fi Protected Access (WPA) em modo de chave pré-compartilhada, devendo ele próprio alterar a frase de senha de cada computador e ponto de acesso sem fio regularmente. Consulte também WPA2-PSK e TKIP.

WPA2

Uma atualização para o padrão de segurança WPA, baseado no padrão 802.11i IEEE.

WPA2-PSK

Um modo WPA especial que é similar ao WPA-PSK e é baseado no padrão WPA2. Um recurso comum do WPA2-PSK é que os dispositivos geralmente suportam vários modos de criptografia (por exemplo, AES, TKIP) simultaneamente, enquanto os dispositivos mais antigos geralmente suportam apenas um único modo de criptografia por vez (ou seja, todos os clientes teriam que usar o mesmo modo de criptografia).

Sobre a McAfee

A McAfee, Inc., com sede em Santa Clara, Califórnia, e líder mundial em prevenção de invasões e gerenciamento de riscos à segurança, fornece soluções e serviços proativos comprovados que protegem sistemas e redes em todo o mundo. Com sua experiência inigualável em segurança e compromisso com a inovação, a McAfee confere a usuários domésticos, empresas públicas e privadas, e provedores de serviços a capacidade de bloquear ataques, evitar problemas e rastrear e aprimorar continuamente sua segurança.

Copyright

Licença

AVISO A TODOS OS USUÁRIOS: LEIA ATENTAMENTE O CONTRATO LEGAL CORRESPONDENTE À LICENÇA ADQUIRIDA POR VOCÊ. NELE ESTÃO DEFINIDOS OS TERMOS E AS CONDIÇÕES GERAIS PARA A UTILIZAÇÃO DO SOFTWARE LICENCIADO. CASO NÃO TENHA CONHECIMENTO DO TIPO DE LICENÇA QUE FOI ADQUIRIDO, CONSULTE A DOCUMENTAÇÃO RELATIVA À COMPRA E VENDA OU À CONCESSÃO DA LICENÇA, INCLUÍDA NO PACOTE DO SOFTWARE OU FORNECIDA SEPARADAMENTE (COMO LIVRETO, ARQUIVO NO CD DO PRODUTO OU UM ARQUIVO DISPONÍVEL NO SITE DO QUAL O PACOTE DE SOFTWARE FOI OBTIDO POR DOWNLOAD). SE NÃO CONCORDAR COM TODOS OS TERMOS ESTABELECIDOS NO CONTRATO, NÃO INSTALE O SOFTWARE. SE FOR APLICÁVEL, VOCÊ PODE DEVOLVER O PRODUTO À MCAFEE, INC. OU AO LOCAL DE AQUISIÇÃO PARA OBTER UM REEMBOLSO TOTAL.

CAPÍTULO 32

Atendimento ao cliente e suporte técnico

O SecurityCenter relata problemas de proteção cruciais e não cruciais assim que os detecta. Os problemas de proteção cruciais exigem ação imediata e comprometem o status da proteção (alterando a cor para vermelho). Os problemas de proteção não cruciais não exigem ação imediata e podem ou não comprometer o status da proteção (dependendo do tipo de problema). Para obter um status de proteção verde, corrija todos os problemas importantes e corrija ou ignore todos os problemas não cruciais. Se você precisar ajudar a diagnosticar os problemas de proteção, poderá executar o McAfee Virtual Technician. Para obter mais informações sobre o McAfee Virtual Technician, consulte a ajuda do McAfee Virtual Technician.

Se você adquiriu seu software de segurança de outro parceiro ou fornecedor e não diretamente da McAfee, abra um navegador da Web e vá para www.mcafeeajuda.com. Em seguida, em Links de Parceiros, selecione o parceiro ou o fornecedor para acessar o McAfee Virtual Technician.

Observação: Para instalar e executar o McAfee Virtual Technician, você terá que efetuar logon no computador como um Administrador do Windows. Caso contrário, talvez o MVT não consiga resolver seus problemas. Para obter informações sobre como efetuar logon como Administrador do Windows, consulte a Ajuda do Windows. No Windows Vista™, você receberá essa solicitação quando executar o MVT. Quando isso acontecer, clique em **Aceitar**. O Virtual Technician não funciona com Mozilla® Firefox.

Neste capítulo

Utilizando o McAfee Virtual Technician

Assim como um representante pessoal do suporte técnico, o Virtual Technician coleta informações sobre os programas do SecurityCenter, para que ele possa resolver os problemas de proteção de seu computador. Quando você executa o Virtual Technician, ele verifica se seus programas do SecurityCenter estão funcionando corretamente. Se detectar problemas, o Virtual Technician oferecerá a opção de corrigi-los para você ou de fornecer informações mais detalhadas sobre eles. Ao concluir, o Virtual Technician exibe os resultados de sua análise e permite que você procure suporte técnico adicional da McAfee, se necessário.

Para manter a segurança e a integridade do computador e de seus arquivos, o Virtual Technician não coleta informações pessoais identificáveis.

Observação: Para obter mais informações sobre o Virtual Technician, clique no ícone da **Ajuda** no Virtual Technician.

Iniciar Virtual Technician

O Virtual Technician coleta informações sobre os programas do SecurityCenter, para que ele possa resolver os seus problemas de proteção. Para proteger sua privacidade, essas informações não incluem informações pessoais identificáveis.

1. Em **Tarefas comuns**, clique em **McAfee Virtual Technician**.
2. Siga as instruções da tela para fazer o download e executar o Virtual Technician.

Suporte e downloads

Consulte as tabelas a seguir para obter os sites de suporte e download da McAfee em seu país, incluindo os Guias de usuário.

Suporte e downloads

País	Suporte técnico da McAfee	Downloads da McAfee
Austrália	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canadá (inglês)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canadá (francês)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
China (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
China (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
República Tcheca	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Dinamarca	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlândia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
França	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Alemanha	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Grã-Bretanha	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Itália	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japão	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Coréia	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
México	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Noruega	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polônia	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Espanha	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Suécia	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turquia	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Estados Unidos	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Guias de usuário do McAfee Total Protection

País	Guias de usuário da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canadá (inglês)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canadá (francês)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
República Tcheca	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Coréia	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polônia	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Guias de usuário do McAfee Internet Security

País	Guias de usuário da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canadá (inglês)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canadá (francês)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
República Tcheca	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Coréia	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polônia	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Guias de usuário do McAfee VirusScan Plus

País	Guias de usuário da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canadá (inglês)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canadá (francês)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
República Tcheca	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Dinamarca	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Coréia	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polônia	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Guias de usuário do McAfee VirusScan

País	Guias de usuário da McAfee
Austrália	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canadá (inglês)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Canadá (francês)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
República Tcheca	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlândia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
França	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Alemanha	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Grã-Bretanha	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Holanda	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Itália	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japão	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Coréia	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polônia	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Espanha	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Suécia	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turquia	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Consulte a seguir a tabela com os sites do McAfee Threat Center e de informações sobre vírus em seu país.

País	Escritório de segurança	Informações sobre vírus
Austrália	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canadá (inglês)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canadá (francês)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
China (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
República Tcheca	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Dinamarca	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlândia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
França	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Alemanha	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Grã-Bretanha	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Holanda	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Itália	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japão	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Coréia	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
México	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Noruega	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polônia	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo

Espanha	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Suécia	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turquia	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Estados Unidos	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Consulte a tabela a seguir para obter os sites do HackerWatch em seu país.

País	HackerWatch
Austrália	www.hackerwatch.org
Brasil	www.hackerwatch.org/?lang=pt-br
Canadá (inglês)	www.hackerwatch.org
Canadá (francês)	www.hackerwatch.org/?lang=fr-ca
China (chn)	www.hackerwatch.org/?lang=zh-cn
China (tw)	www.hackerwatch.org/?lang=zh-tw
República Tcheca	www.hackerwatch.org/?lang=cs
Dinamarca	www.hackerwatch.org/?lang=da
Finlândia	www.hackerwatch.org/?lang=fi
França	www.hackerwatch.org/?lang=fr
Alemanha	www.hackerwatch.org/?lang=de
Grã-Bretanha	www.hackerwatch.org
Holanda	www.hackerwatch.org/?lang=nl
Itália	www.hackerwatch.org/?lang=it
Japão	www.hackerwatch.org/?lang=jp
Coréia	www.hackerwatch.org/?lang=ko
México	www.hackerwatch.org/?lang=es-mx
Noruega	www.hackerwatch.org/?lang=no
Polônia	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Espanha	www.hackerwatch.org/?lang=es
Suécia	www.hackerwatch.org/?lang=sv
Turquia	www.hackerwatch.org/?lang=tr

Estados Unidos	www.hackerwatch.org

Índice

D

E

F

G

O

P

Q

R